



Hewlett Packard
Enterprise

HPE FlexNetwork MSR Router Series

Comware 7 Security Configuration Guide

Part number: 5998-8838a
Software version: CMW710-R0305
Document version: 6PW106-20160621

© Copyright 2016 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

Configuring AAA	1
Overview	1
RADIUS	2
HWTACACS	7
LDAP	9
AAA implementation on the device	12
AAA for MPLS L3VPNs	14
Protocols and standards	14
RADIUS attributes	15
Command and hardware compatibility	18
FIPS compliance	18
AAA configuration considerations and task list	18
Configuring AAA schemes	19
Configuring local users	20
Configuring RADIUS schemes	25
Configuring HWTACACS schemes	36
Configuring LDAP schemes	42
Configuring AAA methods for ISP domains	46
Configuration prerequisites	46
Creating an ISP domain	46
Configuring ISP domain attributes	47
Configuring authentication methods for an ISP domain	49
Configuring authorization methods for an ISP domain	51
Configuring accounting methods for an ISP domain	52
Enabling the session-control feature	54
Configuring the RADIUS DAE server feature	55
Changing the DSCP priority for RADIUS packets	55
Setting the maximum number of concurrent login users	56
Configuring and applying an ITA policy	56
Configuring a NAS-ID profile	57
Configuring the Acct-Session-Id format	57
Displaying and maintaining AAA	58
AAA configuration examples	58
Authentication and authorization for SSH users by a RADIUS server	58
Local authentication and authorization for SSH users	62
AAA for SSH users by an HWTACACS server	63
Authentication for SSH users by an LDAP server	65
Authentication and authorization for SSL VPN users by an LDAP server	70
AAA for PPP users by an HWTACACS server	75
Troubleshooting RADIUS	76
RADIUS authentication failure	76
RADIUS packet delivery failure	77
RADIUS accounting error	77
Troubleshooting HWTACACS	78
Troubleshooting LDAP	78
802.1X overview	79
802.1X architecture	79
Controlled/uncontrolled port and port authorization status	79
802.1X-related protocols	80
Packet formats	80
EAP over RADIUS	81
802.1X authentication initiation	82
802.1X client as the initiator	82
Access device as the initiator	82
802.1X authentication procedures	83
Comparing EAP relay and EAP termination	84

EAP relay	84
EAP termination	86
Configuring 802.1X	88
Access control methods	88
802.1X VLAN manipulation	88
Authorization VLAN	88
Guest VLAN	90
Auth-Fail VLAN	91
Critical VLAN	91
Using 802.1X authentication with other features	92
ACL assignment	92
EAD assistant	93
SmartOn	93
Compatibility information	94
Feature and hardware compatibility	94
Command and hardware compatibility	94
Configuration prerequisites	95
802.1X configuration task list	95
Enabling 802.1X	95
Enabling EAP relay or EAP termination	96
Setting the port authorization state	96
Specifying an access control method	97
Setting the maximum number of concurrent 802.1X users on a port	98
Setting the maximum number of authentication request attempts	98
Setting the 802.1X authentication timeout timers	98
Configuring the online user handshake feature	99
Configuration guidelines	99
Configuration procedure	99
Configuring the authentication trigger feature	100
Configuration guidelines	100
Configuration procedure	100
Specifying a mandatory authentication domain on a port	100
Setting the quiet timer	101
Enabling the periodic online user reauthentication feature	101
Configuring an 802.1X guest VLAN	102
Configuration guidelines	102
Configuration procedure	102
Configuring an 802.1X Auth-Fail VLAN	102
Configuration guidelines	102
Configuration procedure	103
Configuring an 802.1X critical VLAN	103
Configuration guidelines	103
Configuration procedure	103
Specifying supported domain name delimiters	103
Configuring the EAD assistant feature	104
Configuring 802.1X SmartOn	105
Displaying and maintaining 802.1X	106
802.1X authentication configuration examples	106
Basic 802.1X authentication configuration example	106
802.1X guest VLAN and authorization VLAN configuration example	108
802.1X with ACL assignment configuration example	111
802.1X with EAD assistant configuration example (with DHCP relay agent)	112
802.1X with EAD assistant configuration example (with DHCP server)	115
802.1X SmartOn configuration example	117
Troubleshooting 802.1X	119
Web browser users cannot be redirected correctly	119
Configuring MAC authentication	120
Overview	120
User account policies	120
Authentication methods	120

VLAN assignment.....	121
ACL assignment.....	121
Periodic MAC reauthentication	121
Compatibility information	122
Feature and hardware compatibility.....	122
Command and hardware compatibility	122
Configuration prerequisites	122
Configuration task list.....	123
Enabling MAC authentication.....	123
Specifying a MAC authentication domain	123
Configuring the user account format.....	124
Configuring MAC authentication timers	124
Setting the maximum number of concurrent MAC authentication users on a port	125
Configuring MAC authentication delay	125
Enabling MAC authentication multi-VLAN mode on a port.....	126
Configuring the keep-online feature	126
Displaying and maintaining MAC authentication	127
MAC authentication configuration examples	127
Local MAC authentication configuration example	127
RADIUS-based MAC authentication configuration example	129
ACL assignment configuration example	131
Configuring portal authentication	134
Overview.....	134
Extended portal functions.....	134
Portal system components	134
Interaction between portal system components.....	136
Portal authentication modes	136
Portal authentication process.....	137
Command and hardware compatibility.....	139
Portal configuration task list.....	139
Configuration prerequisites	140
Configuring a portal authentication server	140
Configuring a portal Web server	141
Enabling portal authentication on an interface	141
Configuration restrictions and guidelines	142
Configuration procedure	142
Referencing a portal Web server for an interface	142
Controlling portal user access.....	143
Configuring a portal-free rule	143
Configuring an authentication source subnet.....	144
Configuring an authentication destination subnet.....	145
Setting the maximum number of portal users.....	145
Specifying a portal authentication domain	146
Specifying a preauthentication domain	147
Configuring a preauthentication IP address pool for portal users.....	148
Enabling strict-checking on portal authorization information	148
Enabling outgoing packets filtering on a portal-enabled interface	149
Configuring portal detection features.....	149
Configuring online detection of portal users.....	149
Configuring portal authentication server detection	150
Configuring portal Web server detection.....	151
Configuring portal user synchronization.....	152
Configuring the portal fail-permit feature	153
Configuring BAS-IP for portal packets sent to the portal authentication server	153
Enabling portal roaming.....	154
Specifying a format for the NAS-Port-ID attribute	154
Logging out portal users	155
Configuring Web redirect	155
Applying a NAS-ID profile to an interface	156
Displaying and maintaining portal	156
Portal configuration examples.....	157

Configuring direct portal authentication	157
Configuring re-DHCP portal authentication	167
Configuring cross-subnet portal authentication	170
Configuring extended direct portal authentication	173
Configuring extended re-DHCP portal authentication	176
Configuring extended cross-subnet portal authentication	180
Configuring portal server detection and portal user synchronization	184
Configuring cross-subnet portal authentication for MPLS L3VPNs	192
Configuring direct portal authentication with a preauthentication domain	194
Configuring re-DHCP portal authentication with a preauthentication domain	196
Troubleshooting portal	199
No portal authentication page is pushed for users	199
Cannot log out portal users on the access device	199
Cannot log out portal users on the RADIUS server	200
Users logged out by the access device still exist on the portal authentication server	200
Re-DHCP portal authenticated users cannot log in successfully	200
Configuring port security	202
Overview	202
Port security features	202
Port security modes	202
Feature and hardware compatibility	205
Configuration task list	205
Enabling port security	205
Setting port security's limit on the number of secure MAC addresses on a port	206
Setting the port security mode	206
Configuring port security features	208
Configuring NTK	208
Configuring intrusion protection	208
Configuring secure MAC addresses	209
Configuration prerequisites	210
Configuration procedure	210
Ignoring authorization information from the server	211
Enabling MAC move	211
Enabling the authorization-fail-offline feature	212
Applying a NAS-ID profile to port security	212
Displaying and maintaining port security	213
Port security configuration examples	213
autoLearn configuration example	213
userLoginWithOUI configuration example	215
macAddressElseUserLoginSecure configuration example	218
Troubleshooting port security	222
Cannot set the port security mode	222
Cannot configure secure MAC addresses	222
Configuring user profiles	223
Overview	223
Compatibility information	223
Feature and hardware compatibility	223
Command and hardware compatibility	223
User profile configuration task list	223
Configuration restrictions and guidelines	224
Configuring a user profile	224
Displaying and maintaining user profiles	224
Configuring password control	225
Overview	225
Password setting	225
Password updating and expiration	226
User login control	227
Password not displayed in any form	227
Logging	227

FIPS compliance	228
Password control configuration task list	228
Enabling password control	228
Setting global password control parameters	229
Setting user group password control parameters	230
Setting local user password control parameters	231
Setting super password control parameters	231
Displaying and maintaining password control	232
Password control configuration example	232
Network requirements	232
Configuration procedure	233
Verifying the configuration	234
Managing public keys	236
Overview	236
FIPS compliance	236
Creating a local key pair	236
Distributing a local host public key	237
Exporting a host public key	238
Displaying a host public key	238
Destroying a local key pair	238
Configuring a peer host public key	239
Importing a peer host public key from a public key file	239
Entering a peer host public key	239
Displaying and maintaining public keys	240
Examples of public key management	240
Example for entering a peer host public key	240
Example for importing a public key from a public key file	242
Configuring PKI	245
Overview	245
PKI terminology	245
PKI architecture	246
PKI operation	246
PKI applications	247
Support for MPLS L3VPN	247
FIPS compliance	248
PKI configuration task list	248
Configuring a PKI entity	248
Configuring a PKI domain	249
Requesting a certificate	251
Configuration guidelines	251
Configuring automatic certificate request	252
Manually requesting a certificate	252
Aborting a certificate request	253
Obtaining certificates	253
Configuration prerequisites	253
Configuration guidelines	254
Configuration procedure	254
Verifying PKI certificates	254
Verifying certificates with CRL checking	254
Verifying certificates without CRL checking	255
Specifying the storage path for the certificates and CRLs	256
Exporting certificates	256
Removing a certificate	257
Configuring a certificate-based access control policy	257
Displaying and maintaining PKI	258
PKI configuration examples	259
Requesting a certificate from an RSA Keon CA server	259
Requesting a certificate from a Windows Server 2003 CA server	261
Requesting a certificate from an OpenCA server	265
Requesting a certificate from an RSA Keon CA server in an NAT-PT network	268

IKE negotiation with RSA digital signature from a Windows Server 2003 CA server	271
Certificate-based access control policy configuration example	274
Certificate import and export configuration example	275
Troubleshooting PKI configuration	281
Failed to obtain the CA certificate	281
Failed to obtain local certificates	281
Failed to request local certificates	282
Failed to obtain CRLs	283
Failed to import the CA certificate	283
Failed to import a local certificate	284
Failed to export certificates	284
Failed to set the storage path	285
Configuring IPsec	286
Overview	286
Security protocols and encapsulation modes	286
Security association	288
Authentication and encryption	288
IPsec implementation	289
IPsec RRI	290
Protocols and standards	291
FIPS compliance	291
Security strength	291
IPsec tunnel establishment	291
Implementing ACL-based IPsec	292
Configuring an ACL	292
Configuring an IPsec transform set	295
Configuring a manual IPsec policy	297
Configuring an IKE-based IPsec policy	299
Applying an IPsec policy to an interface	303
Enabling ACL checking for de-encapsulated packets	304
Configuring IPsec anti-replay	305
Configuring IPsec anti-replay redundancy	305
Binding a source interface to an IPsec policy	306
Enabling QoS pre-classify	307
Enabling logging of IPsec packets	307
Configuring the DF bit of IPsec packets	307
Configuring IPsec RRI	308
Configuring IPsec for IPv6 routing protocols	309
Configuration task list	309
Configuring a manual IPsec profile	309
Configuring IPsec for tunnels	311
Configuration task list	311
Configuring an IKE-based IPsec profile	311
Applying an IKE-based IPsec profile to a tunnel interface	312
Configuring SNMP notifications for IPsec	312
Displaying and maintaining IPsec	313
IPsec configuration examples	314
Configuring a manual mode IPsec tunnel for IPv4 packets	314
Configuring an IKE-based IPsec tunnel for IPv4 packets	317
Configuring an IKE-based IPsec tunnel for IPv6 packets	320
Configuring IPsec for RIPng	324
Configuring IPsec RRI	327
Configuring IKE	331
Overview	331
IKE negotiation process	331
IKE security mechanism	332
Protocols and standards	333
FIPS compliance	333
IKE configuration prerequisites	333
IKE configuration task list	333

Configuring an IKE profile	334
Configuring an IKE proposal	336
Configuring an IKE keychain	337
Configuring the global identity information	338
Configuring the IKE keepalive function	339
Configuring the IKE NAT keepalive function	339
Configuring IKE DPD	340
Enabling invalid SPI recovery	340
Setting the maximum number of IKE SAs	341
Configuring SNMP notifications for IKE	341
Displaying and maintaining IKE	342
IKE configuration examples	342
Main mode IKE with pre-shared key authentication configuration example	342
Aggressive mode with RSA signature authentication configuration example	346
Aggressive mode with NAT traversal configuration example	353
Troubleshooting IKE	358
IKE negotiation failed because no matching IKE proposals were found	358
IKE negotiation failed because no IKE proposals or IKE keychains are specified correctly	358
IPsec SA negotiation failed because no matching IPsec transform sets were found	359
IPsec SA negotiation failed due to invalid identity information	359
Configuring IKEv2	363
Overview	363
IKEv2 negotiation process	363
New features in IKEv2	364
Protocols and standards	364
IKEv2 configuration task list	364
Configuring an IKEv2 profile	365
Configuring an IKEv2 policy	368
Configuring an IKEv2 proposal	369
Configuring an IKEv2 keychain	370
Configure global IKEv2 parameters	371
Enabling the cookie challenging feature	371
Configuring the IKEv2 DPD feature	371
Configuring the IKEv2 NAT keepalive feature	372
Configuring IKEv2 address pools	372
Displaying and maintaining IKEv2	372
IKEv2 configuration examples	373
IKEv2 with pre-shared key authentication configuration example	373
IKEv2 with RSA signature authentication configuration example	377
IKEv2 with NAT traversal configuration example	385
Troubleshooting IKEv2	390
IKEv2 negotiation failed because no matching IKEv2 proposals were found	390
IPsec SA negotiation failed because no matching IPsec transform sets were found	390
IPsec tunnel establishment failed	391
Configuring SSH	392
Overview	392
How SSH works	392
SSH authentication methods	393
SSH support for Suite B	394
Protocols and standards	394
FIPS compliance	395
Configuring the device as an SSH server	395
SSH server configuration task list	395
Generating local DSA or RSA key pairs	395
Enabling the Stelnet server	396
Enabling the SFTP server	396
Enabling the SCP server	397
Enabling NETCONF over SSH	397
Configuring the user lines for SSH login	397
Configuring a client's host public key	398

Configuring an SSH user	399
Configuring the SSH management parameters	400
Specifying a PKI domain for the SSH server.....	401
Configuring the device as an Stelnet client	402
Stelnet client configuration task list.....	402
Generating local DSA or RSA key pairs.....	402
Specifying the source IP address for SSH packets	402
Establishing a connection to an Stelnet server	403
Establishing a connection to an Stelnet server based on Suite B	406
Configuring the device as an SFTP client	406
SFTP client configuration task list	406
Generating local DSA or RSA key pairs.....	406
Specifying the source IP address for SFTP packets	407
Establishing a connection to an SFTP server.....	407
Establishing a connection to an SFTP server based on Suite B	409
Working with SFTP directories	410
Working with SFTP files.....	410
Displaying help information.....	411
Terminating the connection with the SFTP server.....	411
Configuring the device as an SCP client	411
SCP client configuration task list.....	411
Generating local DSA or RSA key pairs.....	411
Establishing a connection to an SCP server	412
Establishing a connection to an SCP server based on Suite B	415
Specifying algorithms for SSH2.....	415
Specifying key exchange algorithms for SSH2	415
Specifying public key algorithms for SSH2	416
Specifying encryption algorithms for SSH2.....	416
Specifying MAC algorithms for SSH2.....	416
Displaying and maintaining SSH	417
Stelnet configuration examples	417
Password authentication enabled Stelnet server configuration example	417
Publickey authentication enabled Stelnet server configuration example.....	420
Password authentication enabled Stelnet client configuration example	425
Publickey authentication enabled Stelnet client configuration example	429
Stelnet configuration example based on 128-bit Suite B algorithms	431
SFTP configuration examples	435
Password authentication enabled SFTP server configuration example	435
Publickey authentication enabled SFTP client configuration example	437
SFTP configuration example based on 192-bit Suite B algorithms.....	440
SCP configuration examples	444
SCP configuration example with password authentication	444
SCP configuration example based on Suite B algorithms	446
NETCONF over SSH configuration example	453
Network requirements	453
Configuration procedure	453
Verifying the configuration	454
Configuring SSL.....	455
Overview.....	455
SSL security services	455
SSL protocol stack.....	455
FIPS compliance.....	456
SSL configuration task list.....	456
Configuring an SSL server policy.....	456
Configuring an SSL client policy	458
Displaying and maintaining SSL	459
SSL server policy configuration example	459
Configuring ASPF	462
Overview.....	462
ASPF basic concepts	462

ASPF inspections	463
Command and hardware compatibility	465
ASPF configuration task list	465
Configuring an ASPF policy	465
Applying an ASPF policy to an interface	466
Applying an ASPF policy to a zone pair	466
Displaying and maintaining ASPF	467
ASPF configuration examples	467
ASPF FTP application inspection configuration example	467
ASPF TCP application inspection configuration example	468
ASPF H.323 application inspection configuration example	470
ASPF application to a zone pair configuration example	471
Configuring APR	474
Overview	474
PBAR	474
Group-based application recognition	474
Command and hardware compatibility	475
Configuring PBAR	475
Configuring application groups	476
Enabling application statistics on an interface	476
Displaying and maintaining APR	477
APR configuration example	478
Network requirements	478
Configuration procedure	478
Verifying the configuration	478
Managing sessions	479
Overview	479
Session management operation	479
Session management functions	479
Command and hardware compatibility	480
Session management task list	480
Setting the session aging time for different protocol states	480
Setting the session aging time for different application layer protocols	481
Specifying persistent sessions	482
Enabling session statistics collection	482
Configuring session logging	482
Displaying and maintaining session management	483
Configuring connection limits	486
Command and hardware compatibility	486
Interface-based connection limit configuration task list	486
Creating a connection limit policy	487
Configuring the connection limit policy	487
Applying the connection limit policy	488
Displaying and maintaining connection limits	488
Connection limit configuration example	489
Network requirements	489
Configuration procedure	490
Verifying the configuration	491
Troubleshooting connection limits	491
ACLs in the connection limit rules with overlapping segments	491
Configuring object groups	493
Overview	493
Configuring an IPv4 address object group	493
Configuring an IPv6 address object group	493
Configuring a port object group	494
Configuring a service object group	494
Displaying and maintaining object groups	494

Configuring object policies	495
Overview	495
Object policy rules	495
Rule numbering	495
Rule match order	495
Rule description	495
Object policy configuration task list	495
Configuration prerequisites	496
Creating object policies	496
Creating an IPv4 object policy	496
Creating an IPv6 object policy	496
Configuring object policy rules	496
Configuring an IPv4 object policy rule	496
Configuring an IPv6 object policy rule	497
Applying object policies to zone pairs	498
Changing the rule match order	498
Enabling rule matching acceleration	498
Displaying and maintaining object policies	499
Object policy configuration example	499
Network requirements	499
Configuration procedure	500
Verifying the configuration	502
Configuring attack detection and prevention	503
Overview	503
Command and hardware compatibility	503
Attacks that the device can prevent	503
Single-packet attacks	503
Scanning attacks	505
Flood attacks	505
TCP fragment attacks	506
Blacklist feature	506
Client verification	507
TCP client verification	507
DNS client verification	509
HTTP client verification	510
Attack detection and prevention configuration task list	511
Configuring an attack defense policy	511
Creating an attack defense policy	511
Configuring a single-packet attack defense policy	511
Configuring a scanning attack defense policy	513
Configuring a flood attack defense policy	513
Configuring attack detection exemption	518
Applying an attack defense policy to an interface	519
Applying an attack defense policy to the device	519
Disabling log aggregation for single-packet attack events	520
Configuring TCP fragment attack prevention	520
Configuring TCP client verification	520
Configuring DNS client verification	521
Configuring HTTP client verification	522
Configuring the blacklist feature	522
Displaying and maintaining attack detection and prevention	523
Attack detection and prevention configuration examples	528
Interface-based attack detection and prevention configuration example	528
Blacklist configuration example	531
TCP client verification configuration example	532
DNS client verification configuration example	533
HTTP client verification configuration example	534
Configuring IP source guard	536
Overview	536

Static IPSPG bindings	536
Dynamic IPSPG bindings	537
IPSPG configuration task list	537
Configuring the IPv4SPG feature	537
Enabling IPv4SPG on an interface	538
Configuring a static IPv4SPG binding	538
Configuring the IPv6SPG feature	538
Enabling IPv6SPG on an interface	538
Configuring a static IPv6SPG binding	539
Displaying and maintaining IPSPG	539
IPSPG configuration examples	540
Static IPv4SPG configuration example	540
Dynamic IPv4SPG using DHCP snooping configuration example	541
Dynamic IPv4SPG using DHCP relay configuration example	542
Static IPv6SPG configuration example	543
Dynamic IPv6SPG using DHCPv6 snooping configuration example	544
Configuring ARP attack protection	546
Command and hardware compatibility	546
ARP attack protection configuration task list	546
Configuring unresolvable IP attack protection	547
Configuring ARP source suppression	547
Enabling ARP blackhole routing	547
Displaying and maintaining unresolvable IP attack protection	547
Configuration example	548
Configuring source MAC-based ARP attack detection	549
Configuration procedure	549
Displaying and maintaining source MAC-based ARP attack detection	549
Configuration example	550
Configuring ARP packet source MAC consistency check	551
Configuring ARP active acknowledgement	551
Configuring authorized ARP	551
Configuration procedure	552
Configuration example (on a DHCP server)	552
Configuration example (on a DHCP relay agent)	553
Configuring ARP detection	554
Configuring user validity check	555
Configuring ARP packet validity check	556
Configuring ARP restricted forwarding	556
Displaying and maintaining ARP detection	557
User validity check and ARP packet validity check configuration example	557
ARP restricted forwarding configuration example	558
Configuring ARP scanning and fixed ARP	560
Configuration restrictions and guidelines	560
Configuration procedure	560
Configuring ARP gateway protection	561
Configuration guidelines	561
Configuration procedure	561
Configuration example	561
Configuring ARP filtering	562
Configuration guidelines	562
Configuration procedure	562
Configuration example	563
Configuring uRPF	564
Overview	564
uRPF check modes	564
Features	564
uRPF operation	565
Network application	568
Command and hardware compatibility	568
Configuring uRPF	568

Displaying and maintaining uRPF	569
uRPF configuration example	569
Configuring IPv6 uRPF	571
Overview	571
IPv6 uRPF check modes	571
Features	571
IPv6 uRPF operation	572
Network application	574
Command and hardware compatibility	574
Configuring IPv6 uRPF	574
Displaying and maintaining IPv6 uRPF	575
IPv6 uRPF configuration example	575
Configuring crypto engines	577
Overview	577
Command and hardware compatibility	577
Configuring hardware crypto engines	577
Displaying and maintaining crypto engines	578
Configuring FIPS	579
Overview	579
Configuration restrictions and guidelines	579
Configuring FIPS mode	580
Entering FIPS mode	580
Configuration changes in FIPS mode	581
Exiting FIPS mode	582
FIPS self-tests	583
Power-up self-tests	583
Conditional self-tests	583
Triggering self-tests	584
Displaying and maintaining FIPS	584
FIPS configuration examples	584
Entering FIPS mode through automatic reboot	584
Entering FIPS mode through manual reboot	585
Exiting FIPS mode through automatic reboot	587
Exiting FIPS mode through manual reboot	587
Configuring mGRE	589
Overview	589
mGRE operation scheme	589
mGRE operation procedure	589
mGRE support for NAT traversal	592
mGRE configuration task list	592
Configuring an mGRE tunnel	592
Configuring routing	593
Configuring IPsec for an mGRE tunnel	593
Displaying and maintaining mGRE	594
mGRE configuration examples	594
Full-mesh mGRE network configuration example	594
NHS-NHC mGRE network configuration example	598
IPsec-protected full-mesh mGRE network configuration example	601
IPsec-protected NHS-NHC mGRE network configuration example	607
Full-mesh mGRE network with NAT traversal configuration example	612
Document conventions and icons	618
Conventions	618
Network topology icons	619
Support and other resources	620
Accessing Hewlett Packard Enterprise Support	620
Accessing updates	620

Websites	621
Customer self repair.....	621
Remote support	621
Documentation feedback	621
Index	623

Configuring AAA

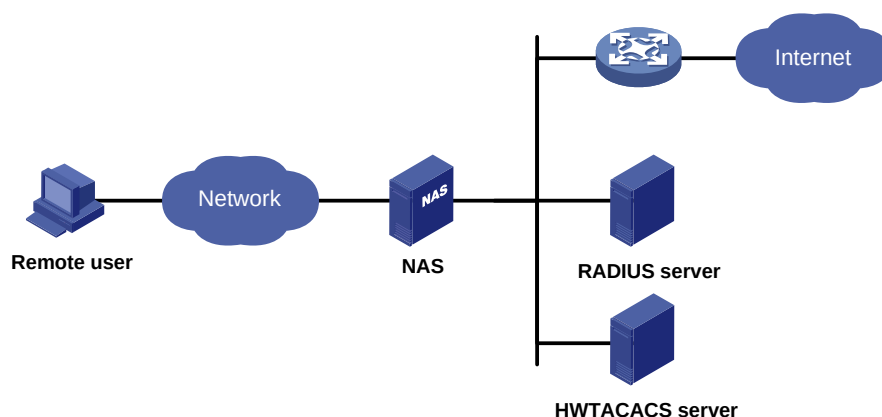
Overview

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. This feature specifies the following security functions:

- **Authentication**—Identifies users and verifies their validity.
- **Authorization**—Grants different users different rights, and controls the users' access to resources and services. For example, you can permit office users to read and print files and prevent guests from accessing files on the device.
- **Accounting**—Records network usage details of users, including the service type, start time, and traffic. This function enables time-based and traffic-based charging and user behavior auditing.

AAA uses a client/server model. The client runs on the access device, or the network access server (NAS), which authenticates user identities and controls user access. The server maintains user information centrally. See [Figure 1](#).

Figure 1 AAA network diagram



To access networks or resources beyond the NAS, a user sends its identity information to the NAS. The NAS transparently passes the user information to AAA servers and waits for the authentication, authorization, and accounting result. Based on the result, the NAS determines whether to permit or deny the access request.

AAA has various implementations, including RADIUS, HWTACACS, and LDAP. RADIUS is most often used.

The network in [Figure 1](#) has one RADIUS server and one HWTACACS server. You can use different servers to implement different security functions. For example, you can use the HWTACACS server for authentication and authorization, and use the RADIUS server for accounting.

You can choose the security functions provided by AAA as needed. For example, if your company wants employees to be authenticated before they access specific resources, you would deploy an authentication server. If network usage information is needed, you would also configure an accounting server.

The device performs dynamic password authentication.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model. The protocol can protect networks against unauthorized access and is often used in network environments that require both high security and remote user access.

The RADIUS authorization process is combined with the RADIUS authentication process, and user authorization information is piggybacked in authentication responses. RADIUS uses UDP port 1812 for authentication and UDP port 1813 for accounting.

RADIUS was originally designed for dial-in user access, and has been extended to support additional access methods, such as Ethernet and ADSL.

Client/server model

The RADIUS client runs on the NASs located throughout the network. It passes user information to RADIUS servers and acts on the responses to, for example, reject or accept user access requests.

The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access.

The RADIUS server operates using the following process:

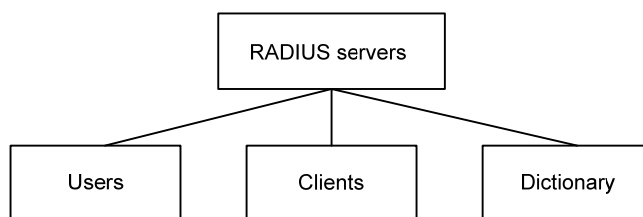
1. Receives authentication, authorization, and accounting requests from RADIUS clients.
2. Performs user authentication, authorization, or accounting.
3. Returns user access control information (for example, rejecting or accepting the user access request) to the clients.

The RADIUS server can also act as the client of another RADIUS server to provide authentication proxy services.

The RADIUS server maintains the following databases:

- **Users**—Stores user information, such as the usernames, passwords, applied protocols, and IP addresses.
- **Clients**—Stores information about RADIUS clients, such as shared keys and IP addresses.
- **Dictionary**—Stores RADIUS protocol attributes and their values.

Figure 2 RADIUS server databases



Information exchange security mechanism

The RADIUS client and server exchange information between them with the help of shared keys, which are preconfigured on the client and server. A RADIUS packet has a 16-byte field called Authenticator. This field includes a signature generated by using the MD5 algorithm, the shared key, and some other information. The receiver of the packet verifies the signature and accepts the packet only when the signature is correct. This mechanism ensures the security of information exchanged between the RADIUS client and server.

The shared keys are also used to encrypt user passwords that are included in RADIUS packets.

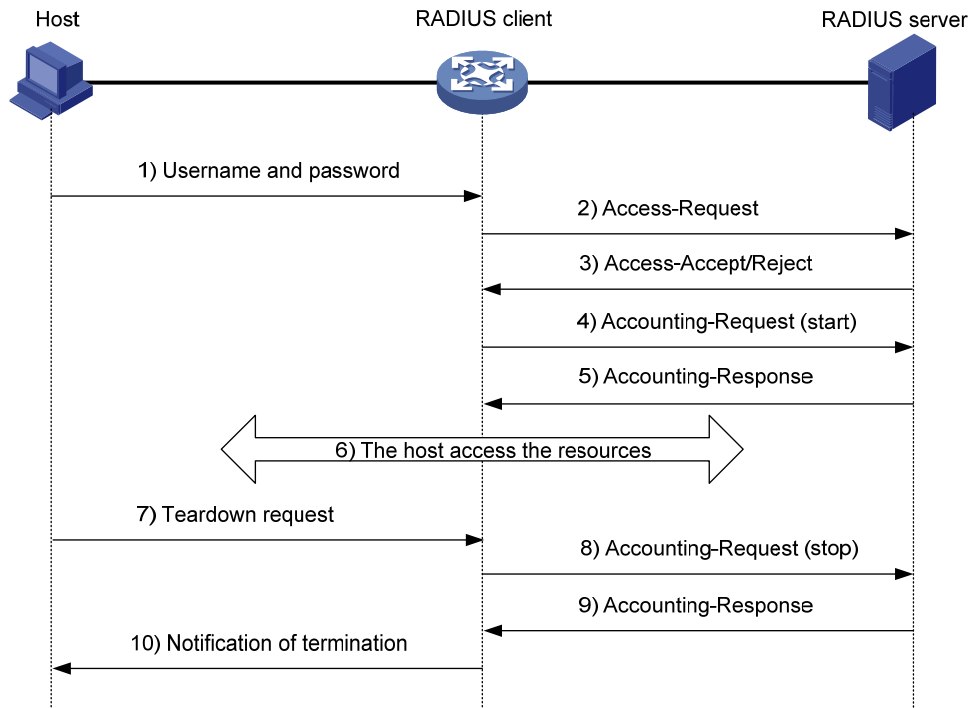
User authentication methods

The RADIUS server supports multiple user authentication methods, such as PAP, CHAP, and EAP.

Basic RADIUS packet exchange process

Figure 3 illustrates the interactions between a user host, the RADIUS client, and the RADIUS server.

Figure 3 Basic RADIUS packet exchange process



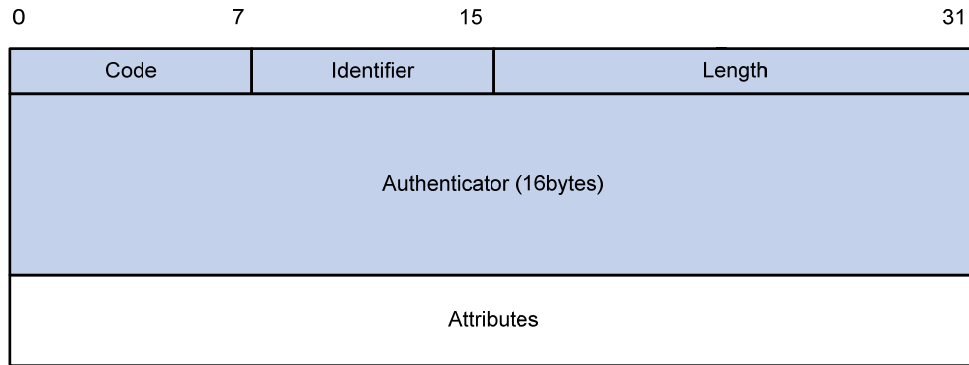
RADIUS uses in the following workflow:

1. The host sends a connection request that includes the user's username and password to the RADIUS client.
2. The RADIUS client sends an authentication request (Access-Request) to the RADIUS server. The request includes the user's password, which has been processed by the MD5 algorithm and shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, the server sends back an Access-Accept packet that contains the user's authorization information. If the authentication fails, the server returns an Access-Reject packet.
4. The RADIUS client permits or denies the user according to the authentication result. If the result permits the user, the RADIUS client sends a start-accounting request (Accounting-Request) packet to the RADIUS server.
5. The RADIUS server returns an acknowledgment (Accounting-Response) packet and starts accounting.
6. The user accesses the network resources.
7. The host requests the RADIUS client to tear down the connection.
8. The RADIUS client sends a stop-accounting request (Accounting-Request) packet to the RADIUS server.
9. The RADIUS server returns an acknowledgment (Accounting-Response) and stops accounting for the user.
10. The RADIUS client notifies the user of the termination.

RADIUS packet format

RADIUS uses UDP to transmit packets. The protocol also uses a series of mechanisms to ensure smooth packet exchange between the RADIUS server and the client. These mechanisms include the timer mechanism, the retransmission mechanism, and the backup server mechanism.

Figure 4 RADIUS packet format



Descriptions of the fields are as follows:

- The Code field (1 byte long) indicates the type of the RADIUS packet. [Table 1](#) gives the main values and their meanings.

Table 1 Main values of the Code field

Code	Packet type	Description
1	Access-Request	From the client to the server. A packet of this type includes user information for the server to authenticate the user. It must contain the User-Name attribute and can optionally contain the attributes of NAS-IP-Address, User-Password, and NAS-Port.
2	Access-Accept	From the server to the client. If all attribute values included in the Access-Request are acceptable, the authentication succeeds, and the server sends an Access-Accept response.
3	Access-Reject	From the server to the client. If any attribute value included in the Access-Request is unacceptable, the authentication fails, and the server sends an Access-Reject response.
4	Accounting-Request	From the client to the server. A packet of this type includes user information for the server to start or stop accounting for the user. The Acct-Status-Type attribute in the packet indicates whether to start or stop accounting.
5	Accounting-Response	From the server to the client. The server sends a packet of this type to notify the client that it has received the Accounting-Request and has successfully recorded the accounting information.

- The Identifier field (1 byte long) is used to match response packets with request packets and to detect duplicate request packets. The request and response packets of the same exchange process for the same purpose (such as authentication or accounting) have the same identifier.
- The Length field (2 bytes long) indicates the length of the entire packet (in bytes), including the Code, Identifier, Length, Authenticator, and Attributes fields. Bytes beyond this length are considered padding and are ignored by the receiver. If the length of a received packet is less than this length, the packet is dropped.
- The Authenticator field (16 bytes long) is used to authenticate responses from the RADIUS server and to encrypt user passwords. There are two types of authenticators: request authenticator and response authenticator.
- The Attributes field (variable in length) includes authentication, authorization, and accounting information. This field can contain multiple attributes, each with the following subfields:

- **Type**—Type of the attribute.
- **Length**—Length of the attribute in bytes, including the Type, Length, and Value subfields.
- **Value**—Value of the attribute. Its format and content depend on the Type subfield.

Commonly used RADIUS attributes are defined in RFC 2865, RFC 2866, RFC 2867, and RFC 2868. For more information, see "[Commonly used standard RADIUS attributes](#)."

Table 2 Commonly used RADIUS attributes

No.	Attribute	No.	Attribute
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token

No.	Attribute	No.	Attribute
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

Extended RADIUS attributes

The RADIUS protocol features excellent extensibility. The Vendor-Specific attribute (attribute 26) allows a vendor to define extended attributes. The extended attributes can implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple subattributes in the TLV format in attribute 26 to provide extended functions. As shown in [Figure 5](#), a subattribute encapsulated in attribute 26 consists of the following parts:

- **Vendor-ID**—ID of the vendor. The most significant byte is 0. The other three bytes contains a code compliant to RFC 1700. The vendor ID of Hewlett Packard Enterprise is 25506.
- **Vendor-Type**—Type of the subattribute.
- **Vendor-Length**—Length of the subattribute.
- **Vendor-Data**—Contents of the subattribute.

For more information about the proprietary RADIUS subattributes of Hewlett Packard Enterprise, see "[Proprietary RADIUS subattributes of Hewlett Packard Enterprise](#)."

Figure 5 Format of attribute 26

0	7	15	23	31
Type		Length		Vendor-ID
Vendor-ID (continued)			Vendor-Type	Vendor-Length
Vendor-Data (Specified attribute value.....)				
.....				

HWTACACS

HW Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). HWTACACS is similar to RADIUS, and uses a client/server model for information exchange between the NAS and the HWTACACS server.

HWTACACS typically provides AAA services for PPP, VPDN, and terminal users. In a typical HWTACACS scenario, terminal users need to log in to the NAS. Working as the HWTACACS client, the NAS sends users' usernames and passwords to the HWTACACS server for authentication. After passing authentication and obtaining authorized rights, a user logs in to the device and performs operations. The HWTACACS server records the operations that each user performs.

Differences between HWTACACS and RADIUS

HWTACACS and RADIUS have many features in common, such as using a client/server model, using shared keys for data encryption, and providing flexibility and scalability. [Table 3](#) lists the primary differences between HWTACACS and RADIUS.

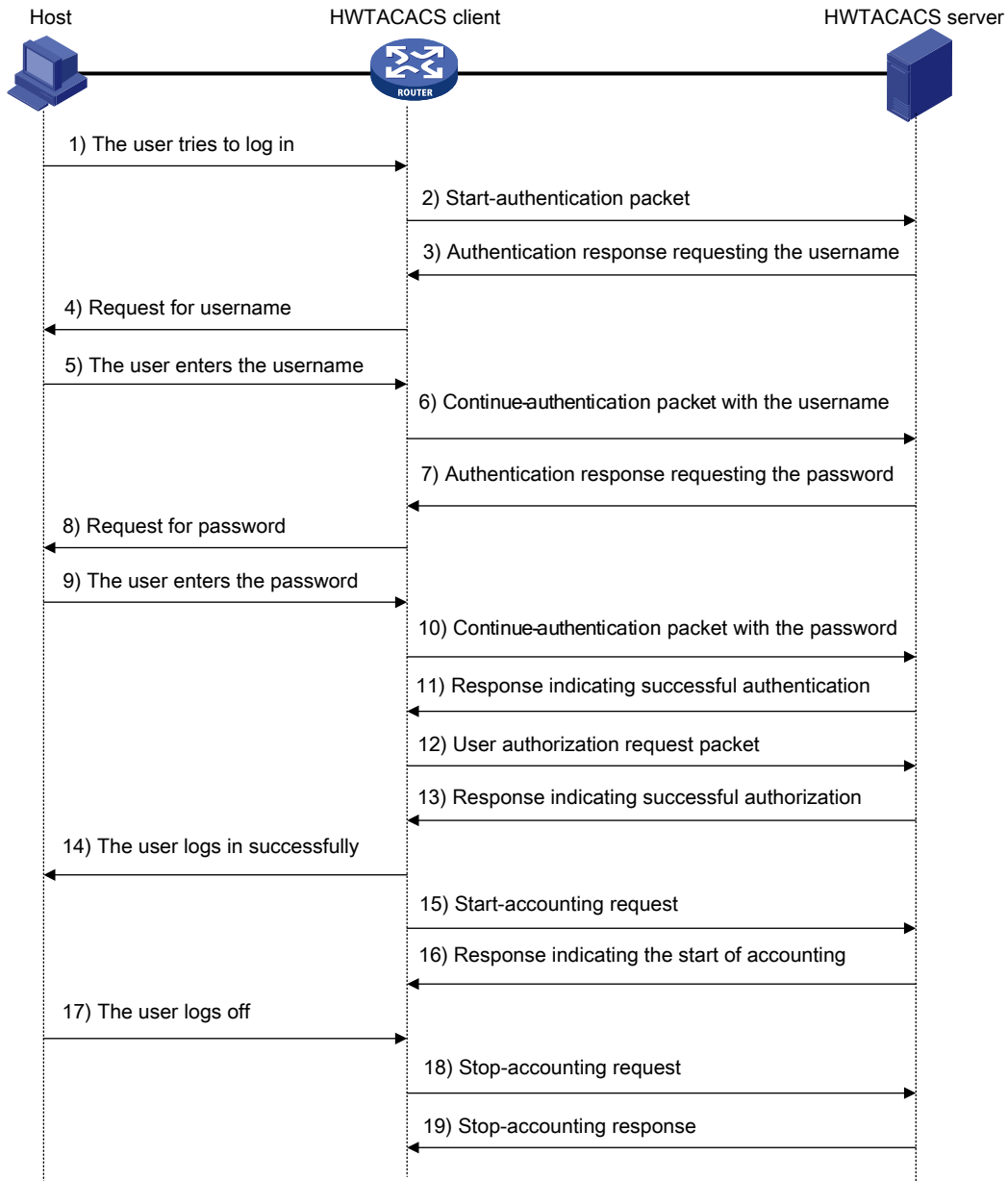
Table 3 Primary differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Uses TCP, which provides reliable network transmission.	Uses UDP, which provides high transport efficiency.
Encrypts the entire packet except for the HWTACACS header.	Encrypts only the user password field in an authentication packet.
Protocol packets are complicated and authorization is independent of authentication. Authentication and authorization can be deployed on different HWTACACS servers.	Protocol packets are simple and the authorization process is combined with the authentication process.
Supports authorization of configuration commands. Access to commands depends on both the user's roles and authorization. A user can use only commands that are permitted by the user roles and authorized by the HWTACACS server.	Does not support authorization of configuration commands. Access to commands solely depends on the user's roles. For more information about user roles, see <i>Fundamentals Configuration Guide</i> .

Basic HWTACACS packet exchange process

[Figure 6](#) describes how HWTACACS performs user authentication, authorization, and accounting for a Telnet user.

Figure 6 Basic HWTACACS packet exchange process for a Telnet user



HWTACACS operates using in the following workflow:

1. A Telnet user sends an access request to the HWTACACS client.
2. The HWTACACS client sends a start-authentication packet to the HWTACACS server when it receives the request.
3. The HWTACACS server sends back an authentication response to request the username.
4. Upon receiving the response, the HWTACACS client asks the user for the username.
5. The user enters the username.
6. After receiving the username from the user, the HWTACACS client sends the server a continue-authentication packet that includes the username.
7. The HWTACACS server sends back an authentication response to request the login password.
8. Upon receipt of the response, the HWTACACS client prompts the user for the login password.
9. The user enters the password.

10. After receiving the login password, the HWTACACS client sends the HWTACACS server a continue-authentication packet that includes the login password.
11. If the authentication succeeds, the HWTACACS server sends back an authentication response to indicate that the user has passed authentication.
12. The HWTACACS client sends a user authorization request packet to the HWTACACS server.
13. If the authorization succeeds, the HWTACACS server sends back an authorization response, indicating that the user is now authorized.
14. Knowing that the user is now authorized, the HWTACACS client pushes its CLI to the user and permits the user to log in.
15. The HWTACACS client sends a start-accounting request to the HWTACACS server.
16. The HWTACACS server sends back an accounting response, indicating that it has received the start-accounting request.
17. The user logs off.
18. The HWTACACS client sends a stop-accounting request to the HWTACACS server.
19. The HWTACACS server sends back a stop-accounting response, indicating that the stop-accounting request has been received.

LDAP

The Lightweight Directory Access Protocol (LDAP) provides standard multiplatform directory service. LDAP was developed on the basis of the X.500 protocol. It improves the following functions of X.500:

- Read/write interactive access.
- Browse.
- Search.

LDAP is suitable for storing data that does not often change. The protocol is used to store user information. For example, LDAP server software Active Directory Server is used in Microsoft Windows operating systems. The software stores the user information and user group information for user login authentication and authorization.

LDAP directory service

LDAP uses directories to maintain the organization information, personnel information, and resource information. The directories are organized in a tree structure and include entries. An entry is a set of attributes with distinguished names (DNs). The attributes are used to store information such as usernames, passwords, emails, computer names, and phone numbers.

LDAP uses a client/server model, and all directory information is stored in the LDAP server. Commonly used LDAP server products include Microsoft Active Directory Server, IBM Tivoli Directory Server, and Sun ONE Directory Server.

LDAP authentication and authorization

AAA can use LDAP to provide authentication and authorization services for users. LDAP defines a set of operations to implement its functions. The main operations for authentication and authorization are the bind operation and search operation.

- The bind operation allows an LDAP client to perform the following operations:
 - Establish a connection with the LDAP server.
 - Obtain the access rights to the LDAP server.
 - Check the validity of user information.
- The search operation constructs search conditions and obtains the directory resource information of the LDAP server.

In LDAP authentication, the client completes the following tasks:

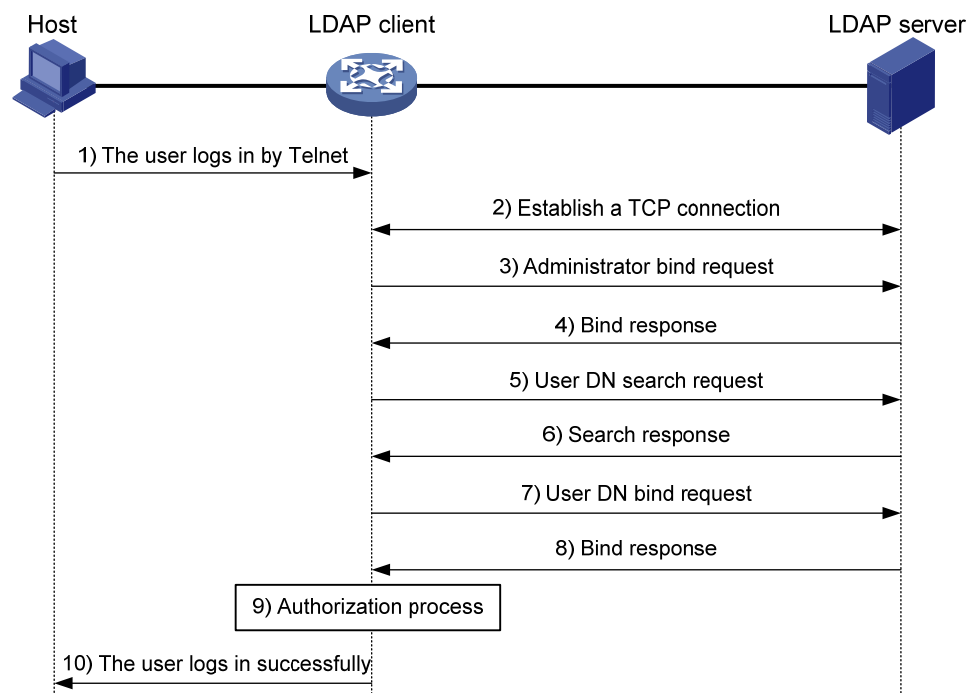
1. Uses the LDAP server administrator DN to bind with the LDAP server. After the binding is created, the client establishes a connection to the server and obtains the right to search.
2. Constructs search conditions by using the username in the authentication information of a user. The specified root directory of the server is searched and a user DN list is generated.
3. Binds with the LDAP server by using each user DN and password. If a binding is created, the user is considered legal.

In LDAP authorization, the client performs the same tasks as in LDAP authentication. When the client constructs search conditions, it obtains both authorization information and the user DN list.

Basic LDAP authentication process

The following example illustrates the basic LDAP authentication process for a Telnet user.

Figure 7 Basic LDAP authentication process for a Telnet user



The following shows the basic LDAP authentication process:

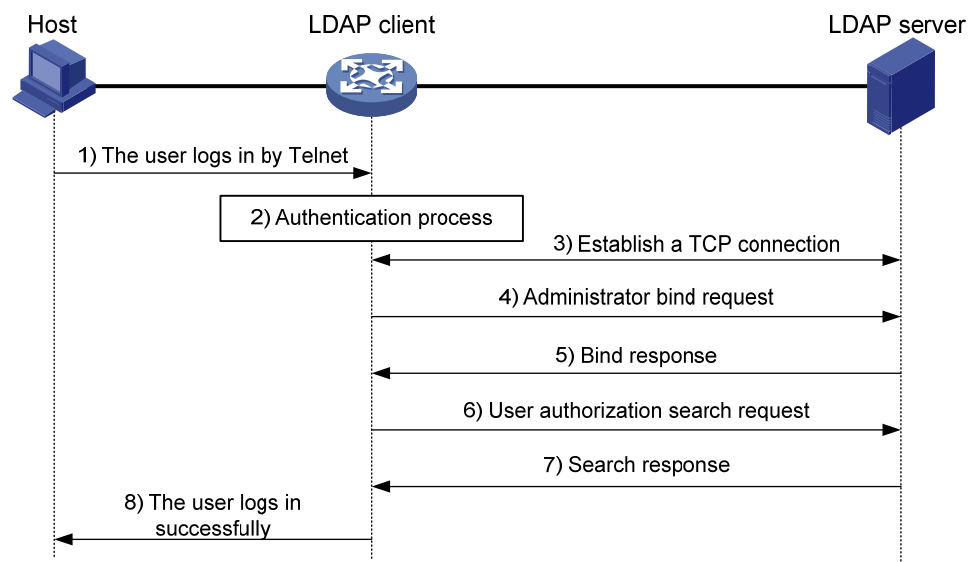
1. A Telnet user initiates a connection request and sends the username and password to the LDAP client.
2. After receiving the request, the LDAP client establishes a TCP connection with the LDAP server.
3. To obtain the right to search, the LDAP client uses the administrator DN and password to send an administrator bind request to the LDAP server.
4. The LDAP server processes the request. If the bind operation is successful, the LDAP server sends an acknowledgment to the LDAP client.
5. The LDAP client sends a user DN search request with the username of the Telnet user to the LDAP server.
6. After receiving the request, the LDAP server searches for the user DN by the base DN, search scope, and filtering conditions. If a match is found, the LDAP server sends a response to notify the LDAP client of the successful search. There might be one or more user DNs found.
7. The LDAP client uses the obtained user DN and the entered user password as parameters to send a user DN bind request to the LDAP server. The server will check whether the user password is correct.

8. The LDAP server processes the request, and sends a response to notify the LDAP client of the bind operation result. If the bind operation fails, the LDAP client uses another obtained user DN as the parameter to send a user DN bind request to the LDAP server. This process continues until a DN is bound successfully or all DNs fail to be bound. If all user DNs fail to be bound, the LDAP client notifies the user of the login failure and denies the user's access request.
9. The LDAP client saves the user DN that has been bound and exchanges authorization packets with the authorization server.
 - If LDAP authorization is used, see the authorization process shown in [Figure 8](#).
 - If another method is expected for authorization, the authorization process of that method applies.
10. After successful authorization, the LDAP client notifies the user of the successful login.

Basic LDAP authorization process

The following example illustrates the basic LDAP authorization process for a Telnet user.

Figure 8 Basic LDAP authorization process for a Telnet user



The following shows the basic LDAP authorization process:

1. A Telnet user initiates a connection request and sends the username and password to the device. The device will act as the LDAP client during authorization.
2. After receiving the request, the device exchanges authentication packets with the authentication server for the user:
 - If LDAP authentication is used, see the authentication process shown in [Figure 7](#).
 - If the device (the LDAP client) uses the same LDAP server for authentication and authorization, skip to step 6.
 - If the device (the LDAP client) uses different LDAP servers for authentication and authorization, skip to step 4.
 - If another authentication method is used, the authentication process of that method applies. The device acts as the LDAP client. Skip to step 3.
3. The LDAP client establishes a TCP connection with the LDAP authorization server.
4. To obtain the right to search, the LDAP client uses the administrator DN and password to send an administrator bind request to the LDAP server.
5. The LDAP server processes the request. If the bind operation is successful, the LDAP server sends an acknowledgment to the LDAP client.

6. The LDAP client sends an authorization search request with the username of the Telnet user to the LDAP server. If the user uses the same LDAP server for authentication and authorization, the client sends the request with the saved user DN of the Telnet user to the LDAP server.
7. After receiving the request, the LDAP server searches for the user information by the base DN, search scope, filtering conditions, and LDAP attributes. If a match is found, the LDAP server sends a response to notify the LDAP client of the successful search.
8. After successful authorization, the LDAP client notifies the user of the successful login.

AAA implementation on the device

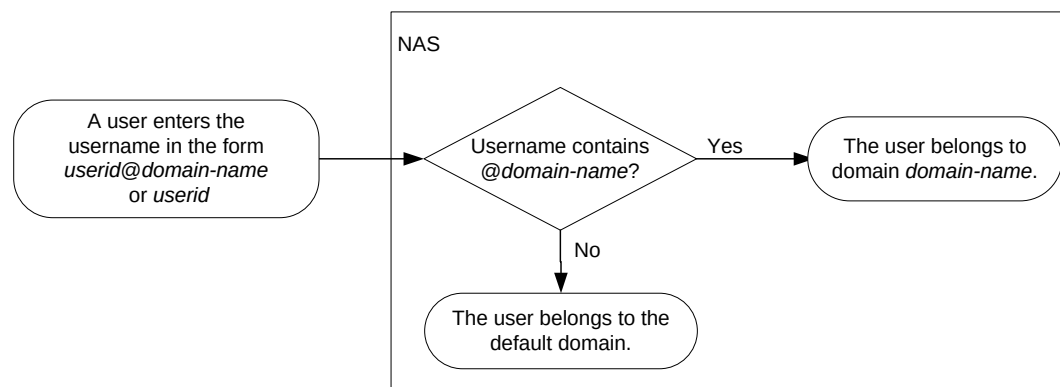
This section describes AAA user management and methods.

User management based on ISP domains and user access types

AAA manages users based on the users' ISP domains and access types.

On a NAS, each user belongs to one ISP domain. The NAS determines the ISP domain to which a user belongs based on the username entered by the user at login.

Figure 9 Determining the ISP domain for a user by username



AAA manages users in the same ISP domain based on the users' access types. The device supports the following user access types:

- **LAN**—LAN users must pass 802.1X or MAC authentication to come online.
- **Login**—Login users include SSH, Telnet, FTP, and terminal users who log in to the device. Terminal users can access through a console, AUX, or Async port.
- **ADVPN**.
- **X.25 PAD**.
- **Portal**—Portal users must pass portal authentication to access the network.
- **PPP**.
- **IPoE**—IPoE users include Layer 2 and Layer 3 leased line users and Set Top Box (STB) users.
- **Web**—Web users log in to the Web interface of the device through HTTP or HTTPS.
- **SSL VPN**.

NOTE:

The device also provides authentication modules (such as 802.1X) for implementation of user authentication management policies. If you configure these authentication modules, the ISP domains for users of the access types depend on the configuration of the authentication modules.

AAA methods

AAA supports configuring different authentication, authorization, and accounting methods for different types of users in an ISP domain. The NAS determines the ISP domain and access type of a user. The NAS also uses the methods configured for the access type in the domain to control the user's access.

AAA also supports configuring a set of default methods for an ISP domain. These default methods are applied to users for whom no AAA methods are configured.

The device supports the following authentication methods:

- **No authentication**—This method trusts all users and does not perform authentication. For security purposes, do not use this method.
- **Local authentication**—The NAS authenticates users by itself, based on the locally configured user information including the usernames, passwords, and attributes. Local authentication allows high speed and low cost, but the amount of information that can be stored is limited by the size of the storage space.
- **Remote authentication**—The NAS works with a RADIUS, HWTACACS, or LDAP server to authenticate users. The server manages user information in a centralized manner. Remote authentication provides high capacity, reliable, and centralized authentication services for multiple NASs. You can configure backup methods to be used when the remote server is not available.

The device supports the following authorization methods:

- **No authorization**—The NAS performs no authorization exchange. The following default authorization information applies after users pass authentication:
 - Non-login users can access the network.
 - Login users obtain the default user role. For more information about the default user role feature, see *Fundamentals Configuration Guide*.
 - FTP, SFTP, and SCP login users also have the root directory of the NAS set as the working directory. However, the users do not have permission to access the root directory.
- **Local authorization**—The NAS performs authorization according to the user attributes locally configured for users.
- **Remote authorization**—The NAS works with a RADIUS, HWTACACS, or LDAP server to authorize users. RADIUS authorization is bound with RADIUS authentication. RADIUS authorization can work only after RADIUS authentication is successful, and the authorization information is included in the Access-Accept packet. HWTACACS authorization is separate from HWTACACS authentication, and the authorization information is included in the authorization response after successful authentication. You can configure backup methods to be used when the remote server is not available.

The device supports the following accounting methods:

- **No accounting**—The NAS does not perform accounting for the users.
- **Local accounting**—Local accounting is implemented on the NAS. It counts and controls the number of concurrent users who use the same local user account, but does not provide statistics for charging.
- **Remote accounting**—The NAS works with a RADIUS server or HWTACACS server for accounting. You can configure backup methods to be used when the remote server is not available.

In addition, the device provides the following login services to enhance device security:

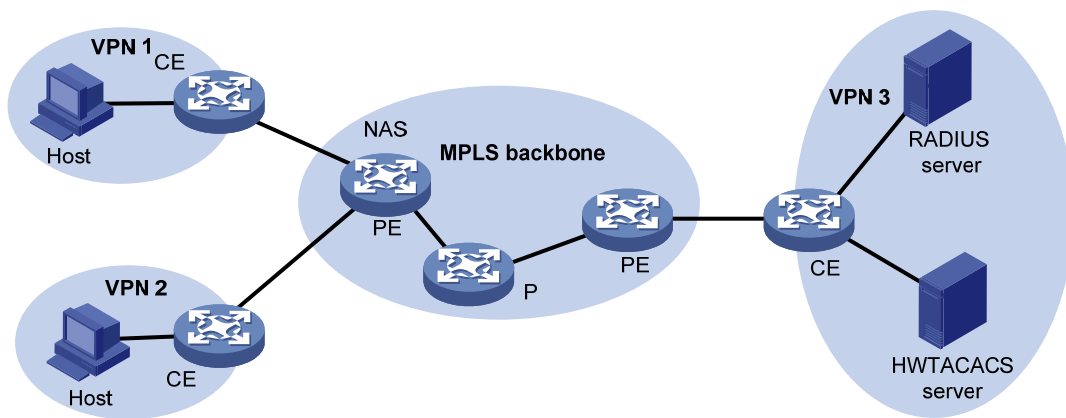
- **Command authorization**—Enables the NAS to let the authorization server determine whether a command entered by a login user is permitted. Login users can execute only commands permitted by the authorization server. For more information about command authorization, see *Fundamentals Configuration Guide*.

- **Command accounting**—When command authorization is disabled, command accounting enables the accounting server to record all valid commands executed on the device. When command authorization is enabled, command accounting enables the accounting server to record all authorized commands. For more information about command accounting, see *Fundamentals Configuration Guide*.
- **User role authentication**—Authenticates each user who wants to obtain another user role without logging out or getting disconnected. For more information about user role authentication, see *Fundamentals Configuration Guide*.

AAA for MPLS L3VPNs

You can deploy AAA across VPNs in an MPLS L3VPN scenario where clients in different VPNs are centrally authenticated. The deployment enables forwarding of RADIUS and HWTACACS packets across MPLS VPNs. For example, as shown in [Figure 10](#), you can deploy AAA across the VPNs. The PE at the left side of the MPLS backbone acts as a NAS. The NAS transparently delivers the AAA packets of private users in VPN 1 and VPN 2 to the AAA servers in VPN 3 for centralized authentication. Authentication packets of private users in different VPNs do not affect each other.

Figure 10 Network diagram



This feature can also help an MCE to implement portal authentication for VPNs. For more information about MCE, see *MPLS Configuration Guide*. For more information about portal authentication, see "[Configuring portal authentication](#)."

Protocols and standards

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
- RFC 1777, *Lightweight Directory Access Protocol*
- RFC 2251, *Lightweight Directory Access Protocol (v3)*

RADIUS attributes

Commonly used standard RADIUS attributes

No.	Attribute	Description
1	User-Name	Name of the user to be authenticated.
2	User-Password	User password for PAP authentication, only present in Access-Request packets when PAP authentication is used.
3	CHAP-Password	Digest of the user password for CHAP authentication, only present in Access-Request packets when CHAP authentication is used.
4	NAS-IP-Address	IP address for the server to use to identify the client. Typically, a client is identified by the IP address of its access interface. This attribute is only present in Access-Request packets.
5	NAS-Port	Physical port of the NAS that the user accesses.
6	Service-Type	Type of service that the user has requested or type of service to be provided.
7	Framed-Protocol	Encapsulation protocol for framed access.
8	Framed-IP-Address	IP address assigned to the user.
11	Filter-ID	Name of the filter list.
12	Framed-MTU	MTU for the data link between the user and NAS. For example, this attribute can be used to define the maximum size of EAP packets allowed to be processed in 802.1X EAP authentication.
14	Login-IP-Host	IP address of the NAS interface that the user accesses.
15	Login-Service	Type of the service that the user uses for login.
18	Reply-Message	Text to be displayed to the user, which can be used by the server to communicate information, for example, the reason of the authentication failure.
26	Vendor-Specific	Vendor-specific proprietary attribute. A packet can contain one or more proprietary attributes, each of which can contain one or more subattributes.
27	Session-Timeout	Maximum service duration for the user before termination of the session.
28	Idle-Timeout	Maximum idle time permitted for the user before termination of the session.
31	Calling-Station-Id	User identification that the NAS sends to the server. For the LAN access service provided by an HPE device, this attribute includes the MAC address of the user in the format HHHH-HHHH-HHHH.
32	NAS-Identifier	Identification that the NAS uses to identify itself to the RADIUS server.

No.	Attribute	Description
40	Acct-Status-Type	Type of the Accounting-Request packet. Possible values include: 1—Start. 2—Stop. 3—Interim-Update. 4—Reset-Charge. 7—Accounting-On. (Defined in the 3rd Generation Partnership Project.) 8—Accounting-Off. (Defined in the 3rd Generation Partnership Project.) 9 to 14—Reserved for tunnel accounting. 15—Reserved for failed.
45	Acct-Authentic	Authentication method used by the user. Possible values include: 1—RADIUS. 2—Local. 3—Remote.
60	CHAP-Challenge	CHAP challenge generated by the NAS for MD5 calculation during CHAP authentication.
61	NAS-Port-Type	Type of the physical port of the NAS that is authenticating the user. Possible values include: 15—Ethernet. 16—Any type of ADSL. 17—Cable. (With cable for cable TV.) 19—WLAN-IEEE 802.11. 201—VLAN. 202—ATM. If the port is an ATM or Ethernet one and VLANs are implemented on it, the value of this attribute is 201.
79	EAP-Message	Used to encapsulate EAP packets to allow RADIUS to support EAP authentication.
80	Message-Authenticator	Used for authentication and verification of authentication packets to prevent spoofing Access-Requests. This attribute is present when EAP authentication is used.
87	NAS-Port-Id	String for describing the port of the NAS that is authenticating the user.

Proprietary RADIUS subattributes of Hewlett Packard Enterprise

No.	Subattribute	Description
1	Input-Peak-Rate	Peak rate in the direction from the user to the NAS, in bps.
2	Input-Average-Rate	Average rate in the direction from the user to the NAS, in bps.
3	Input-Basic-Rate	Basic rate in the direction from the user to the NAS, in bps.
4	Output-Peak-Rate	Peak rate in the direction from the NAS to the user, in bps.
5	Output-Average-Rate	Average rate in the direction from the NAS to the user, in bps.
6	Output-Basic-Rate	Basic rate in the direction from the NAS to the user, in bps.
15	Remanent_Volume	Total amount of data available for the connection, in different units for different server types.

No.	Subattribute	Description
20	Command	Operation for the session, used for session control. Possible values include: 1—Trigger-Request. 2—Terminate-Request. 3—SetPolicy. 4—Result. 5—PortalClear.
24	Control_Identifier	Identification for retransmitted packets. For retransmitted packets from the same session, this attribute must be the same value. For retransmitted packets from different sessions, this attribute does not have to be the same value. The client response of a retransmitted packet must also include this attribute and the value of this attribute must be the same. For Accounting-Request packets of the start, stop, and interim update types, the Control_Identifier attribute does not take effect.
25	Result_Code	Result of the Trigger-Request or SetPolicy operation, zero for success and any other value for failure.
26	Connect_ID	Index of the user connection.
28	Ftp_Directory	FTP, SFTP, or SCP user working directory. When the RADIUS client acts as the FTP, SFTP, or SCP server, this attribute is used to set the working directory for an FTP, SFTP, or SCP user on the RADIUS client.
29	Exec_Privilege	EXEC user priority.
59	NAS_Startup_Timestamp	Startup time of the NAS in seconds, which is represented by the time elapsed after 00:00:00 on Jan. 1, 1970 (UTC).
60	Ip_Host_Addr	User IP address and MAC address included in authentication and accounting requests, in the format A.B.C.D hh:hh:hh:hh:hh:hh. A space is required between the IP address and the MAC address.
61	User_Notify	Information that must be sent from the server to the client transparently.
62	User_HeartBeat	Hash value assigned after an 802.1X user passes authentication, which is a 32-byte string. This attribute is stored in the user list on the NAS and verifies the handshake packets from the 802.1X user. This attribute only exists in Access-Accept and Accounting-Request packets.
140	User_Group	User groups assigned after the SSL VPN user passes authentication. A user can belong to multiple user groups that are separated by semicolons. This attribute is used to work with the SSL VPN device.
141	Security_Level	Security level assigned after the SSL VPN user passes security authentication.
201	Input-Interval-Octets	Number of bytes input within a real-time accounting interval.
202	Output-Interval-Octets	Number of bytes output within a real-time accounting interval.
203	Input-Interval-Packets	Number of packets input within an accounting interval in the unit set on the NAS.
204	Output-Interval-Packets	Number of packets output within an accounting interval in the unit set on the NAS.
205	Input-Interval-Gigawords	Amount of bytes input within an accounting interval, in units of 4G bytes.

No.	Subattribute	Description
206	Output-Interval-Gigawords	Amount of bytes output within an accounting interval, in units of 4G bytes.
207	Backup-NAS-IP	Backup source IP address for sending RADIUS packets.
255	Product_ID	Product name.

Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

FIPS compliance

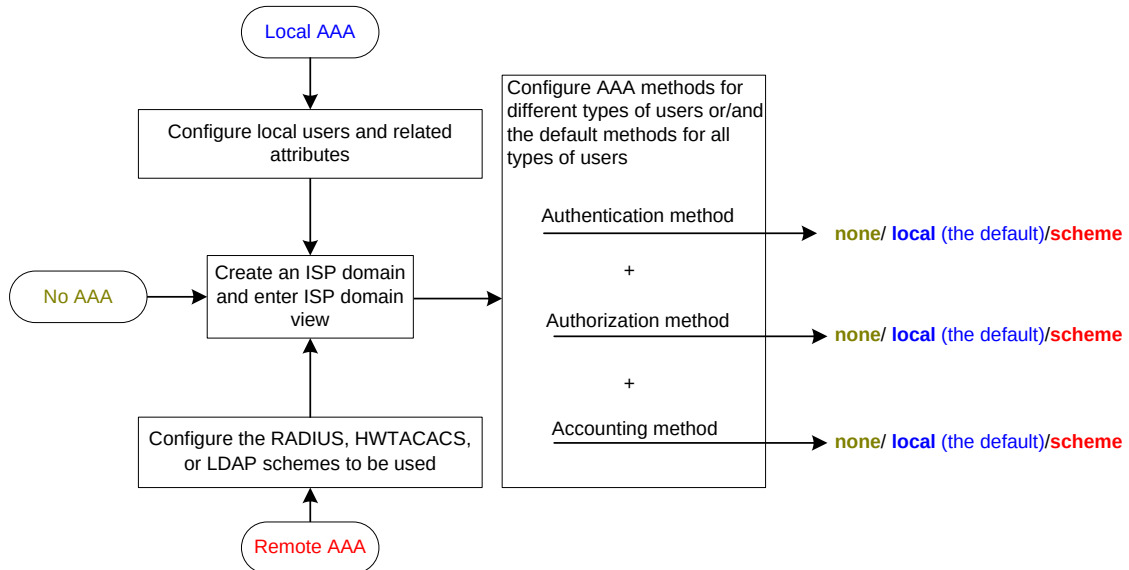
The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "[Configuring FIPS](#)") and non-FIPS mode.

AAA configuration considerations and task list

To configure AAA, complete the following tasks on the NAS:

1. Configure the required AAA schemes:
 - **Local authentication**—Configure local users and the related attributes, including the usernames and passwords, for the users to be authenticated.
 - **Remote authentication**—Configure the required RADIUS, HWTACACS, and LDAP schemes.
2. Configure AAA methods for the users' ISP domains. Remote AAA methods need to use the configured RADIUS, HWTACACS, and LDAP schemes.

Figure 11 AAA configuration procedure



To configure AAA, perform the following tasks:

Tasks at a glance
(Required.) Perform at least one of the following tasks to configure local users or AAA schemes: • Configuring local users • Configuring RADIUS schemes • Configuring HWTACACS schemes • Configuring LDAP schemes
(Required.) Configure AAA methods for ISP domains: 1. (Required.) Creating an ISP domain 2. (Optional.) Configuring ISP domain attributes 3. (Required.) Perform at least one of the following tasks to configure AAA authentication, authorization, and accounting methods for the ISP domain: ○ Configuring authentication methods for an ISP domain ○ Configuring authorization methods for an ISP domain ○ Configuring accounting methods for an ISP domain
(Optional.) Enabling the session-control feature
(Optional.) Configuring the RADIUS DAE server feature
(Optional.) Changing the DSCP priority for RADIUS packets
(Optional.) Setting the maximum number of concurrent login users
(Optional.) Configuring and applying an ITA policy
(Optional.) Configuring a NAS-ID profile
(Optional.) Configuring the Acct-Session-Id format

Configuring AAA schemes

This section includes information on configuring local users, RADIUS schemes, HWTACACS schemes, and LDAP schemes.

Configuring local users

To implement local authentication, authorization, and accounting, create local users and configure user attributes on the device. The local users and attributes are stored in the local user database on the device. A local user is uniquely identified by the combination of a username and a user type. Local users are classified into the following types:

- **Device management user**—User who logs in to the device for device management.
- **Network access user**—User who accesses network resources through the device.

The following shows the configurable local user attributes:

- **Service type**—Services that the user can use. Local authentication checks the service types of a local user. If none of the service types is available, the user cannot pass authentication.
Service types include ADVPN, FTP, HTTP, HTTPS, IPoE, LAN access, PAD, portal, PPP, SSH, SSL VPN, Telnet, and terminal.
- **User state**—Whether or not a local user can request network services. There are two user states: active and blocked. A user in active state can request network services, but a user in blocked state cannot.
- **Upper limit of concurrent logins using the same user name**—Maximum number of users who can concurrently access the device by using the same user name. When the number reaches the upper limit, no more local users can access the device by using the user name.
- **User group**—Each local user belongs to a local user group and has all attributes of the group. The attributes include the password control attributes and authorization attributes. For more information about local user group, see "[Configuring user group attributes](#)."
- **Binding attributes**—Binding attributes control the scope of users, and are checked during local authentication of a user. If the attributes of a user do not match the binding attributes configured for the local user account, the user cannot pass authentication. Binding attributes include the ISDN calling number, IP address, access port, MAC address, and native VLAN. For support and usage information about binding attributes, see "[Configuring local user attributes](#)."
- **Authorization attributes**—Authorization attributes indicate the user's rights after it passes local authentication. Authorization attributes include the ACL, idle cut function, PPP callback number, user profile, user role, VLAN, FTP/SFTP/SCP working directory, VPN instance, and IP service attributes. The IP service attributes include IPv4 address, IPv6 address, IPv6 address prefix, IPv6 address pool, primary or secondary DNS server address, and redirect URL. For support information about authorization attributes, see "[Configuring local user attributes](#)."
Configure the authorization attributes based on the service type of local users. For example, you do not need to configure the FTP/SFTP/SCP working directory attribute for a PPP user.
You can configure an authorization attribute in user group view or local user view. The setting of an authorization attribute in local user view takes precedence over the attribute setting in user group view.
 - The attribute configured in user group view takes effect on all local users in the user group.
 - The attribute configured in local user view takes effect only on the local user.
- **Password control attributes**—Password control attributes help control password security for device management users. Password control attributes include password aging time, minimum password length, password composition checking, password complexity checking, and login attempt limit.
You can configure a password control attribute in system view, user group view, or local user view. A password control attribute with a smaller effective range has a higher priority. For more information about password management and global password configuration, see "[Configuring password control](#)."

Local user configuration task list

Tasks at a glance
(Required.) Configuring local user attributes
(Optional.) Configuring user group attributes
(Optional.) Displaying and maintaining local users and local user groups

Configuring local user attributes

When you configure local user attributes, follow these guidelines:

- When you use the **password-control enable** command to globally enable the password control feature, local user passwords are not displayed.
- You can configure authorization attributes and password control attributes in local user view or user group view. The setting in local user view takes precedence over the setting in user group view.
- Configure authorization attributes according to the application environments and purposes. Support for authorization attributes depends on the service types of users.
 - For PPP users, only the following authorization attributes are effective: **callback-number**, **idle-cut**, **ip**, **ipv6**, **ipv6-pool**, **ipv6-prefix**, **primary-dns**, **secondary-dns**, **url**, **user-profile**, and **vpn-instance**.
 - For IPoE users, only the following authorization attributes are effective: **idle-cut**, **ip**, **ipv6**, **ipv6-pool**, **ipv6-prefix**, **user-profile**, and **vpn-instance**.
 - For portal users, only the following authorization attributes are effective: **acl**, **idle-cut**, **ip**, **ipv6**, **ipv6-pool**, **user-profile**, and **vlan**.
 - For LAN users, only the following authorization attributes are effective: **acl**, **user-profile**, and **vlan**.
 - For HTTP, HTTPS, Telnet, and terminal users, only the authorization attribute **user-role** is effective.
 - For SSH and FTP users, only the authorization attributes **user-role** and **work-directory** are effective.
 - For SSL VPN users, only the authorization attribute **sslvpn-policy-group** is effective.
 - For other types of local users, no authorization attribute is effective.

To configure local user attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Add a local user and enter local user view.	local-user <i>user-name</i> [class { manage network }]	By default, no local user exists.

Step	Command	Remarks
3. (Optional.) Configure a password for the local user.	- For a network access user: password { cipher simple } <i>password</i> - For a device management user: - In non-FIPS mode: password [{ hash simple } <i>password</i>] - In FIPS mode: password	Network access user passwords are encrypted with the encryption algorithm and saved in ciphertext. Device management user passwords are encrypted with the hash algorithm and saved in ciphertext. In non-FIPS mode, a non-password-protected user passes authentication if the user provides the correct username and passes attribute checks. To enhance security, configure a password for each local user. In FIPS mode, only password-protected users can pass authentication.
4. Assign services to the local user.	- For a network access user: service-type { advpn ipoe lan-access portal ppp sslvpn } - For a device management user: - In non-FIPS mode: service-type { ftp { http https pad ssh telnet terminal } * } - In FIPS mode: service-type { https pad ssh terminal } *	By default, no service is authorized to a local user.
5. (Optional.) Place the local user to the active or blocked state.	state { active block }	By default, a created local user is in active state and can request network services.
6. (Optional.) Set the upper limit of concurrent logins using the local user name.	access-limit <i>max-user-number</i>	By default, the number of concurrent logins is not limited for the local user. This command takes effect only when local accounting is configured for the local user. It does not apply to FTP, SFTP, or SCP users, who do not support accounting.
7. (Optional.) Configure binding attributes for the local user.	bind-attribute { call-number <i>call-number</i> [: <i>subcall-number</i>] ip <i>ip-address</i> location interface <i>interface-type interface-number</i> mac <i>mac-address</i> vlan <i>vlan-id</i> } *	By default, no binding attribute is configured for a local user. Binding attribute call-number applies only to PPP users. Binding attribute ip applies only to LAN users using 802.1X. Binding attributes location, mac, and vlan apply only to IPoE, LAN, portal, and PPP users.

Step	Command	Remarks
8. (Optional.) Configure authorization attributes for the local user.	<pre> authorization-attribute { acl acl-number callback-number callback-number idle-cut <i>minute</i> ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> ipv6-pool <i>ipv6-pool-name</i> ipv6-prefix <i>ipv6-prefix</i> <i>prefix-length</i> { primary-dns secondary-dns } { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } sslvpn-policy-group <i>group-name</i> url <i>url-string</i> user-profile <i>profile-name</i> user-role <i>role-name</i> vlan <i>vlan-id</i> vpn-instance <i>vpn-instance-name</i> work-directory <i>directory-name</i> } * </pre>	The following default settings apply: - FTP, SFTP, and SCP users have the root directory of the NAS set as the working directory. However, the users do not have permission to access the root directory. - The network-operator user role is assigned to local users that are created by a network-admin or level-15 user.
9. (Optional.) Configure password control attributes for the local user.	- Set the password aging time: password-control aging <i>aging-time</i> - Set the minimum password length: password-control length <i>length</i> - Configure the password composition policy: password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>] - Configure the password complexity checking policy: password-control complexity { same-character user-name } check - Configure the maximum login attempts and the action to take if there is a login failure: password-control login-attempt <i>login-times</i> [exceed { lock lock-time <i>time</i> unlock }]	By default, the local user uses password control attributes of the user group to which the local user belongs. Only device management users support the password control feature.
10. (Optional.) Assign the local user to a user group.	group <i>group-name</i>	By default, a local user belongs to the default user group system .

Configuring user group attributes

User groups simplify local user configuration and management. A user group contains a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized user attributes management for the local users in the group. Local user attributes that are manageable include authorization attributes.

By default, every new local user belongs to the default user group **system** and has all attributes of the group. To assign a local user to a different user group, use the **group** command in local user view.

To configure user group attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a user group and enter user group view.	user-group <i>group-name</i>	By default, there is a system-defined user group named system , which is the default user group.
3. Configure authorization attributes for the user group.	authorization-attribute { acl <i>acl-number</i> callback-number <i>callback-number</i> idle-cut <i>minute</i> ipv6-pool <i>ipv6-pool-name</i> ipv6-prefix <i>ipv6-prefix</i> <i>prefix-length</i> { primary-dns secondary-dns } { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } sslvpn-policy-group <i>group-name</i> url <i>url-string</i> user-profile <i>profile-name</i> vlan <i>vlan-id</i> vpn-instance <i>vpn-instance-name</i> work-directory <i>directory-name</i> } *	By default, no authorization attribute is configured for a user group.
4. (Optional.) Configure password control attributes for the user group.	- Set the password aging time: password-control aging <i>aging-time</i> - Set the minimum password length: password-control length <i>length</i> - Configure the password composition policy: password-control composition type-number [type-length <i>type-length</i>] - Configure the password complexity checking policy: password-control complexity { same-character user-name } check - Configure the maximum login attempts and the action to take for login failures: password-control login-attempt <i>login-times</i> [exceed { lock lock-time <i>time</i> } unlock] }	By default, the user group uses the global password control settings. For more information, see " Configuring password control ."

Displaying and maintaining local users and local user groups

Execute **display** commands in any view.

Task	Command
Display the local user configuration and online user statistics.	display local-user [class { manage network } idle-cut { disable enable } service-type { advpn ftp http https ipoe lan-access pad portal ppp ssh sslvpn telnet terminal } state { active block } user-name <i>user-name</i> vlan <i>vlan-id</i>]
Display the user group configuration.	display user-group [<i>group-name</i>]

Configuring RADIUS schemes

A RADIUS scheme specifies the RADIUS servers that the device can work with and defines a set of parameters. The device uses the parameters to exchange information with the RADIUS servers, including the server IP addresses, UDP port numbers, shared keys, and server types.

Configuration task list

Tasks at a glance
(Optional.) Configuring a test profile for RADIUS server status detection
(Required.) Creating a RADIUS scheme
(Required.) Specifying the RADIUS authentication servers
(Optional.) Specifying the RADIUS accounting servers and the relevant parameters
(Optional.) Specifying the shared keys for secure RADIUS communication
(Optional.) Specifying a VPN for the scheme
(Optional.) Setting the username format and traffic statistics units
(Optional.) Setting the maximum number of RADIUS request transmission attempts
(Optional.) Setting the status of RADIUS servers
(Optional.) Specifying the source IP address for outgoing RADIUS packets
(Optional.) Setting RADIUS timers
(Optional.) Enabling the accounting-on feature
(Optional.) Enabling the extended accounting-on feature
(Optional.) Configuring the IP addresses of the security policy servers
(Optional.) Interpreting the RADIUS class attribute as CAR parameters
(Optional.) Configuring the Login-Service attribute check method for SSH, FTP, and terminal users
(Optional.) Setting the data measurement unit for the Remanent_Volume attribute
(Optional.) Specifying a HUAWEI attribute version for interpretation of HUAWEI RADIUS attributes 26-1 and 26-4
(Optional.) Enabling SNMP notifications for RADIUS
(Optional.) Displaying and maintaining RADIUS

Configuring a test profile for RADIUS server status detection

Use a test profile to detect whether a RADIUS authentication server is reachable at a detection interval. To detect the RADIUS server status, you must configure the RADIUS server to use this test profile in a RADIUS scheme.

With the test profile specified, the device sends a detection packet to the RADIUS server within each detection interval. The detection packet is a simulated authentication request that includes the specified user name in the test profile.

- If the device receives a response from the server within the interval, it sets the server to the active state.
- If the device does not receive any response from the server within the interval, it sets the server to the blocked state.

The device refreshes the RADIUS server status at each detection interval according to the detection result.

The device stops detecting the status of the RADIUS server when one of the following operations is performed:

- The RADIUS server is removed from the RADIUS scheme.
- The test profile configuration is removed for the RADIUS server in RADIUS scheme view.
- The test profile is deleted.
- The RADIUS server is manually set to the blocked state.
- The RADIUS scheme is deleted.

To configure a test profile for RADIUS server status detection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a test profile for detecting the status of RADIUS authentication servers.	radius-server test-profile <i>profile-name username name</i> [interval <i>interval</i>]	By default, no test profile is created on the device to detect the status of RADIUS servers. You can configure multiple test profiles by executing this command multiple times.

Creating a RADIUS scheme

Create a RADIUS scheme before performing any other RADIUS configurations. You can configure a maximum of 16 RADIUS schemes. A RADIUS scheme can be used by multiple ISP domains.

To create a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a RADIUS scheme and enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	By default, no RADIUS scheme is defined.

Specifying the RADIUS authentication servers

A RADIUS authentication server completes authentication and authorization together, because authorization information is piggybacked in authentication responses sent to RADIUS clients.

You can specify one primary authentication server and a maximum of 16 secondary authentication servers for a RADIUS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. A RADIUS authentication server can function as the primary authentication server for one scheme and a secondary authentication server for another scheme at the same time.

To specify RADIUS authentication servers for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A

Step	Command	Remarks
3. Specify RADIUS authentication servers.	- Specify the primary RADIUS authentication server: primary authentication { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> test-profile <i>profile-name</i> vpn-instance <i>vpn-instance-name</i>] * - Specify a secondary RADIUS authentication server: secondary authentication { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> test-profile <i>profile-name</i> vpn-instance <i>vpn-instance-name</i>] *	By default, no authentication server is specified. To support server status detection, specify an existing test profile for the RADIUS authentication server. If the test profile does not exist, the device cannot detect the server status. Two authentication servers in a scheme, primary or secondary, cannot have the same combination of IP address, port number, and VPN.

Specifying the RADIUS accounting servers and the relevant parameters

You can specify one primary accounting server and a maximum of 16 secondary accounting servers for a RADIUS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. A RADIUS accounting server can function as the primary accounting server for one scheme and a secondary accounting server for another scheme at the same time.

The device sends a stop-accounting request to the accounting server in the following situations:

- The device receives a connection teardown request from a host.
- The device receives a connection teardown command from an administrator.

When the maximum number of real-time accounting attempts is reached, the device disconnects users who have no accounting responses.

RADIUS does not support accounting for FTP, SFTP, and SCP users.

To specify RADIUS accounting servers and the relevant parameters for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify RADIUS accounting servers.	- Specify the primary RADIUS accounting server: primary accounting { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> vpn-instance <i>vpn-instance-name</i>] * - Specify a secondary RADIUS accounting server: secondary accounting { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> vpn-instance <i>vpn-instance-name</i>] *	By default, no accounting server is specified. Two accounting servers in a scheme, primary or secondary, cannot have the same combination of IP address, port number, and VPN.

Step	Command	Remarks
4. (Optional.) Set the maximum number of real-time accounting attempts.	retry realtime-accounting <i>retry-times</i>	The default setting is 5.

Specifying the shared keys for secure RADIUS communication

The RADIUS client and server use the MD5 algorithm and shared keys to generate the Authenticator value for packet authentication and user password encryption. The client and server must use the same key for each type of communication.

A key configured in this task is for all servers of the same type (accounting or authentication) in the scheme. The key has a lower priority than a key configured individually for a RADIUS server.

To specify a shared key for secure RADIUS communication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify a shared key for secure RADIUS communication.	key { accounting authentication } { cipher simple } string	By default, no shared key is specified. The shared key configured on the device must be the same as that configured on the RADIUS server.

Specifying a VPN for the scheme

The VPN specified for a RADIUS scheme applies to all authentication and accounting servers in that scheme. If a VPN is also configured for an individual RADIUS server, the VPN specified for the RADIUS scheme does not take effect on that server.

To specify a VPN for a scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify a VPN for the RADIUS scheme.	vpn-instance <i>vpn-instance-name</i>	By default, a RADIUS scheme belongs to the public network.

Setting the username format and traffic statistics units

A username is in the *userid@isp-name* format, where the *isp-name* argument represents the user's ISP domain name. By default, the ISP domain name is included in a username. However, older RADIUS servers might not recognize usernames that contain the ISP domain names. In this case, you can configure the device to remove the domain name of each username to be sent.

If two or more ISP domains use the same RADIUS scheme, configure the RADIUS scheme to keep the ISP domain name in usernames for domain identification.

The device reports online user traffic statistics in accounting packets. The traffic measurement units are configurable, but they must be the same as the traffic measurement units configured on the RADIUS accounting servers.

To set the username format and the traffic statistics units for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Set the format for usernames sent to the RADIUS servers.	user-name-format { keep-original with-domain without-domain }	By default, the ISP domain name is included in a username.
4. (Optional.) Set the data flow and packet measurement units for traffic statistics.	data-flow-format { data { byte giga-byte kilo-byte mega-byte } packet { giga-packet kilo-packet mega-packet one-packet } }*	By default, traffic is counted in bytes and packets.

Setting the maximum number of RADIUS request transmission attempts

RADIUS uses UDP packets to transfer data. Because UDP communication is not reliable, RADIUS uses a retransmission mechanism to improve reliability. A RADIUS request is retransmitted if the NAS does not receive a server response for the request within the response timeout timer. For more information about the RADIUS server response timeout timer, see "[Setting RADIUS timers](#)."

You can set the maximum number for the NAS to retransmit a RADIUS request to the same server. When the maximum number is reached, the NAS tries to communicate with other RADIUS servers in active state. If no other servers are in active state at the time, the NAS considers the authentication or accounting attempt a failure.

To set the maximum number of RADIUS request transmission attempts:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Set the maximum number of RADIUS request transmission attempts.	retry <i>retry-times</i>	The default setting is 3.

Setting the status of RADIUS servers

To control the RADIUS servers with which the device communicates when the current servers are no longer available, set the status of RADIUS servers to blocked or active. You can specify one primary RADIUS server and multiple secondary RADIUS servers. The secondary servers function as the backup of the primary server. The device chooses servers based on the following rules:

- When the primary server is in active state, the device communicates with the primary server.
- If the primary server fails, the device performs the following operations:
 - Changes the server status to blocked.
 - Starts a quiet timer for the server.
 - Tries to communicate with a secondary server in active state that has the highest priority.
- If the secondary server is unreachable, the device performs the following operations:
 - Changes the server status to blocked.
 - Starts a quiet timer for the server.
 - Tries to communicate with the next secondary server in active state that has the highest priority.

- The search process continues until the device finds an available secondary server or has checked all secondary servers in active state. If no server is available, the device considers the authentication or accounting attempt a failure.
- When the quiet timer of a server expires or you manually set the server to the active state, the status of the server changes back to active. The device does not check the server again during the authentication or accounting process.
- When you remove a server in use, communication with the server times out. The device looks for a server in active state by first checking the primary server, and then checking secondary servers in the order they are configured.
- When all servers are in blocked state, the device only tries to communicate with the primary server.
- When one or more servers are in active state, the device tries to communicate with these active servers only, even if the servers are unavailable.
- When a RADIUS server's status changes automatically, the device changes this server's status accordingly in all RADIUS schemes in which this server is specified.
- When a RADIUS server is manually set to blocked, server detection is disabled for the server, regardless of whether a test profile has been specified for the server. When the RADIUS server is set to active state, server detection is enabled for the server on which an existing test profile is specified.

By default, the device sets the status of all RADIUS servers to active. However, in some situations, you must change the status of a server. For example, if a server fails, you can change the status of the server to blocked to avoid communication attempts to the server.

To set the status of RADIUS servers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Set the RADIUS server status.	• Set the status of the primary RADIUS authentication server: state primary authentication { active block } • Set the status of the primary RADIUS accounting server: state primary accounting { active block } • Set the status of a secondary RADIUS authentication server: state secondary authentication [{ ipv4-address ipv6 ipv6-address } [port-number vpn-instance vpn-instance-name] *] { active block } • Set the status of a secondary RADIUS accounting server: state secondary accounting [{ ipv4-address ipv6 ipv6-address } [port-number vpn-instance vpn-instance-name] *] { active block }	By default, every server specified in a RADIUS scheme is in active state. The configured server status cannot be saved to any configuration file, and can only be viewed by using the display radius scheme command. After the device restarts, all servers are restored to the active state.

Specifying the source IP address for outgoing RADIUS packets

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon

receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of a managed NAS.

- If it is the IP address of a managed NAS, the server processes the packet.
- If it is not the IP address of a managed NAS, the server drops the packet.

The source address of outgoing RADIUS packets is typically the IP address of an egress interface on the NAS to communicate with the RADIUS server. However, in some situations, you must change the source IP address. For example, when VRRP is configured for stateful failover, configure the virtual IP of the uplink VRRP group as the source address.

You can specify a source IP address for outgoing RADIUS packets in RADIUS scheme view or in system view.

- The IP address specified in RADIUS scheme view applies only to one RADIUS scheme.
- The IP address specified in system view applies to all RADIUS schemes whose servers are in a VPN or the public network.

Before sending a RADIUS packet, the NAS selects a source IP address in the following order:

1. The source IP address specified for the RADIUS scheme.
2. The source IP address specified in system view for the VPN or public network, depending on where the RADIUS server resides.
3. The IP address of the outbound interface specified by the route.

To specify a source IP address for all RADIUS schemes in a VPN or the public network:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a source IP address for outgoing RADIUS packets.	radius nas-ip { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]	By default, the IP address of the RADIUS packet outbound interface is used as the source IP address.

To specify a source IP address for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify a source IP address for outgoing RADIUS packets.	nas-ip { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	By default, the source IP address specified by the radius nas-ip command in system view is used. If the source IP address is not specified, the IP address of the outbound interface is used.

Setting RADIUS timers

The device uses the following types of timers to control communication with a RADIUS server:

- **Server response timeout timer (response-timeout)**—Defines the RADIUS request retransmission interval. The timer starts immediately after a RADIUS request is sent. If the device does not receive a response from the RADIUS server before the timer expires, it resends the request.
- **Server quiet timer (quiet)**—Defines the duration to keep an unreachable server in blocked state. If one server is not reachable, the device changes the server status to blocked, starts this timer for the server, and tries to communicate with another server in active state. After the server quiet timer expires, the device changes the status of the server back to active.

- **Real-time accounting timer (realtime-accounting)**—Defines the interval at which the device sends real-time accounting packets to the RADIUS accounting server for online users.

When you set RADIUS timers, follow these guidelines:

- When you configure the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer, consider the number of secondary servers. If the retransmission process takes too much time, the client connection in the access module (for example, Telnet) might time out during the process.
- When a number of secondary servers are configured, the client connections of access modules that have a short client connection timeout period might still be timed out during initial authentication or accounting, even if the packet transmission attempt limit and server response timeout period are configured with small values. However, the next authentication or accounting attempt can succeed, because the device has set the unreachable servers to blocked, which shortens the amount of time for finding a reachable server.
- Make sure the server quiet timer is set correctly. A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state. A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.
- A short real-time accounting interval helps improve accounting precision but requires many system resources. When there are 1000 or more users, set the interval to 15 minutes or longer.

To set RADIUS timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Set the RADIUS server response timeout timer.	timer response-timeout <i>seconds</i>	The default setting is 3 seconds.
4. Set the quiet timer for the servers.	timer quiet <i>minutes</i>	The default setting is 5 minutes.
5. Set the real-time accounting timer.	timer realtime-accounting <i>minutes interval [second]</i>	The default setting is 12 minutes.

Enabling the accounting-on feature

The accounting-on feature enables the device to automatically send an accounting-on packet to the RADIUS server after a device or card reboot. Upon receiving the accounting-on packet, the RADIUS server logs out all online users who log in through the device or card. Without this feature, users cannot log in again after the device or card reboot, because the RADIUS server considers them to come online.

You can configure the interval for which the device waits to resend the accounting-on packet and the maximum number of retries.

The RADIUS server must run on IMC to correctly log out users when a card reboots on the distributed device to which the users connect.

To enable the accounting-on feature for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A

Step	Command	Remarks
3. Enable accounting-on.	accounting-on enable [interval seconds send send-times] *	By default, the accounting-on feature is disabled.

Enabling the extended accounting-on feature

This feature enhances the accounting-on feature. It takes effect on a distributed device whose SPUs are rebooted without the reboot of the whole device.

The extended accounting-on feature enables the device to automatically send an extended accounting-on packet to the RADIUS server after an SPU reboot. Upon receiving the extended accounting-on packet, the RADIUS server logs out all online users who access the device through the SPU.

This feature requires the RADIUS server to run on IMC.

For the extended accounting-on feature to take effect, you must enable the accounting-on feature.

The extended accounting-on feature is applicable to IPoE, LAN, and PPP users. The feature is not applicable to portal users, because all portal user information is saved on MPUs.

To enable the extended accounting-on feature for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Enable extended accounting-on.	accounting-on extended	By default, the extended accounting-on feature is disabled.

Configuring the IP addresses of the security policy servers

The NAS verifies the validity of received control packets and accepts only control packets from known servers. To use a security policy server that is independent of the AAA servers, configure the IP address of the security policy server on the NAS.

The security policy server is the management and control center of the HPE EAD solution. To implement all EAD functions, configure both the IP address of the security policy server and that of the IMC Platform on the NAS.

To configure the IP address of a security policy server for a scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify a security policy server.	security-policy-server { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]	By default, no security policy server is specified for a scheme. You can specify a maximum of eight security policy servers for a RADIUS scheme.

Interpreting the RADIUS class attribute as CAR parameters

A RADIUS server might deliver CAR parameters for user-based traffic monitoring and control by using the RADIUS class attribute (attribute 25). You can configure the device to interpret the class attribute to CAR parameters in the RADIUS packets to be forwarded to users.

To configure the device to interpret the RADIUS class attribute as CAR parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Interpret the RADIUS class attribute as CAR parameters.	attribute 25 car	By default, the RADIUS class attribute is not interpreted.

Configuring the Login-Service attribute check method for SSH, FTP, and terminal users

The device supports the following check methods for the Login-Service attribute (RADIUS attribute 15) of SSH, FTP, and terminal users:

- **Strict**—Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively.
- **Loose**—Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.

An Access-Accept packet received for a user must contain the matching attribute value. Otherwise, the user cannot log in to the device.

Use the loose check method only when the server does not issue Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal users.

To configure the Login-Service attribute check method for SSH, FTP, and terminal users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Configure the Login-Service attribute check method for SSH, FTP, and terminal users.	attribute 15 check-mode { loose strict }	The default check method is strict .

Setting the data measurement unit for the Remanent_Volume attribute

The Remanent_Volume attribute is Hewlett Packard Enterprise proprietary. The RADIUS server uses this attribute in authentication or real-time accounting responses to notify the device of the current amount of data available for online users.

Perform this task to set the data measurement unit for the Remanent_Volume attribute. Make sure the configured measurement unit is the same as the user data measurement unit on the RADIUS server.

To set the data measurement unit for the Remanent_Volume attribute:

Step	Commands	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Set the data measurement unit for the Remanent_Volume attribute.	attribute remanent-volume unit { byte giga-byte kilo-byte mega-byte }	By default, the data measurement unit is kilobyte.

Specifying a HUAWEI attribute version for interpretation of HUAWEI RADIUS attributes 26-1 and 26-4

Configure the device to interpret HUAWEI RADIUS attributes 26-1 and 26-4 based on the following attribute versions:

- **Version 1.0**—Interprets attribute 26-1 as the input peak rate in bps and attribute 26-4 as the output peak rate in bps.
- **Version 1.1**—Interprets attribute 26-1 as the input committed burst size in bits and attribute 26-4 as the output committed burst size in bits.

For the device to correctly interpret attributes 26-1 and 26-4, the specified attribute version must match the version of the RADIUS server.

To specify a HUAWEI attribute version for the device to interpret attributes 26-1 and 26-4:

Step	Commands	Remarks
1. Enter system view.	system-view	N/A
2. Enter RADIUS scheme view.	radius scheme <i>radius-scheme-name</i>	N/A
3. Specify a HUAWEI RADIUS attribute version.	attribute vendor huawei version { 1.0 1.1 }	By default, version 1.0 is used.

Enabling SNMP notifications for RADIUS

When SNMP notifications are enabled for RADIUS, the SNMP agent supports the following notifications generated by RADIUS:

- **RADIUS server unreachable notification**—The RADIUS server cannot be reached. RADIUS generates this notification if it does not receive a response to an accounting or authentication request within the specified number of RADIUS request transmission attempts.
- **RADIUS server reachable notification**—The RADIUS server can be reached. RADIUS generates this notification for a previously blocked RADIUS server after the quiet timer expires.
- **Excessive authentication failures notification**—The number of authentication failures compared to the total number of authentication attempts exceeds the specified threshold.

You can configure SNMP parameters to control the output of these SNMP notifications. For more information, see *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for RADIUS:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable SNMP notifications for RADIUS.	snmp-agent trap enable radius [accounting-server-down authentication-error-threshold authentication-server-down accounting-server-up authentication-server-up] *	By default, all types of SNMP notifications are disabled for RADIUS.

Displaying and maintaining RADIUS

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the RADIUS scheme configuration.	display radius scheme [<i>radius-scheme-name</i>]
Display RADIUS packet statistics.	display radius statistics

Task	Command
Clear RADIUS statistics.	<code>reset radius statistics</code>

Configuring HWTACACS schemes

Configuration task list

Tasks at a glance
(Required.) Creating an HWTACACS scheme
(Required.) Specifying the HWTACACS authentication servers
(Optional.) Specifying the HWTACACS authorization servers
(Optional.) Specifying the HWTACACS accounting servers
(Required.) Specifying the shared keys for secure HWTACACS communication
(Optional.) Specifying a VPN for the scheme
(Optional.) Setting the username format and traffic statistics units
(Optional.) Specifying the source IP address for outgoing HWTACACS packets
(Optional.) Setting HWTACACS timers
(Optional.) Displaying and maintaining HWTACACS

Creating an HWTACACS scheme

Create an HWTACACS scheme before performing any other HWTACACS configurations. You can configure a maximum of 16 HWTACACS schemes. An HWTACACS scheme can be used by multiple ISP domains.

To create an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	<code>system-view</code>	N/A
2. Create an HWTACACS scheme and enter HWTACACS scheme view.	<code>hwtacacs scheme</code> <code>hwtacacs-scheme-name</code>	By default, no HWTACACS scheme is defined.

Specifying the HWTACACS authentication servers

You can specify one primary authentication server and a maximum of 16 secondary authentication servers for an HWTACACS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary authentication server in one scheme and as the secondary authentication server in another scheme at the same time.

To specify HWTACACS authentication servers for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	<code>system-view</code>	N/A
2. Enter HWTACACS scheme view.	<code>hwtacacs scheme</code> <code>hwtacacs-scheme-name</code>	N/A

Step	Command	Remarks
3. Specify HWTACACS authentication servers.	- Specify the primary HWTACACS authentication server: primary authentication { ipv4-address ipv6 ipv6-address } [port-number key { cipher simple } string single-connection vpn-instance vpn-instance-name] * - Specify a secondary HWTACACS authentication server: secondary authentication { ipv4-address ipv6 ipv6-address } [port-number key { cipher simple } string single-connection vpn-instance vpn-instance-name] *	By default, no authentication server is specified. Two HWTACACS authentication servers in a scheme, primary or secondary, cannot have the same combination of IP address, port number, and VPN.

Specifying the HWTACACS authorization servers

You can specify one primary authorization server and a maximum of 16 secondary authorization servers for an HWTACACS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary authorization server of one scheme and as the secondary authorization server of another scheme at the same time.

To specify HWTACACS authorization servers for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme hwtacacs-scheme-name	N/A
3. Specify HWTACACS authorization servers.	- Specify the primary HWTACACS authorization server: primary authorization { ipv4-address ipv6 ipv6-address } [port-number key { cipher simple } string single-connection vpn-instance vpn-instance-name] * - Specify a secondary HWTACACS authorization server: secondary authorization { ipv4-address ipv6 ipv6-address } [port-number key { cipher simple } string single-connection vpn-instance vpn-instance-name] *	By default, no authorization server is specified. Two HWTACACS authorization servers in a scheme, primary or secondary, cannot have the same combination of IP address, port number, and VPN.

Specifying the HWTACACS accounting servers

You can specify one primary accounting server and a maximum of 16 secondary accounting servers for an HWTACACS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary accounting server of one scheme and as the secondary accounting server of another scheme at the same time.

HWTACACS does not support accounting for FTP, SFTP, and SCP users.

To specify HWTACACS accounting servers for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Specify HWTACACS accounting servers.	- Specify the primary HWTACACS accounting server: primary accounting { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> single-connection vpn-instance <i>vpn-instance-name</i>] * - Specify a secondary HWTACACS accounting server: secondary accounting { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key { cipher simple } <i>string</i> single-connection vpn-instance <i>vpn-instance-name</i>] *	By default, no accounting server is specified. Two HWTACACS accounting servers in a scheme, primary or secondary, cannot have the same combination of IP address, port number, and VPN.

Specifying the shared keys for secure HWTACACS communication

The HWTACACS client and server use the MD5 algorithm and shared keys to generate the Authenticator value for packet authentication and user password encryption. The client and server must use the same key for each type of communication.

Perform this task to configure shared keys for servers in an HWTACACS scheme. The keys take effect on all servers for which a shared key is not individually configured.

To specify a shared key for secure HWTACACS communication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Specify a shared key for secure HWTACACS authentication, authorization, or accounting communication.	key { accounting authentication authorization } { cipher simple } <i>string</i>	By default, no shared key is specified. The shared key configured on the device must be the same as that configured on the HWTACACS server.

Specifying a VPN for the scheme

The VPN specified for an HWTACACS scheme applies to all servers in that scheme. If a VPN is also configured for an individual HWTACACS server, the VPN specified for the HWTACACS scheme does not take effect on that server.

To specify a VPN for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Specify a VPN for the HWTACACS scheme.	vpn-instance <i>vpn-instance-name</i>	By default, an HWTACACS scheme belongs to the public network.

Setting the username format and traffic statistics units

A username is typically in the *userid@isp-name* format, where the *isp-name* argument represents the user's ISP domain name. By default, the ISP domain name is included in a username. If HWTACACS servers do not recognize usernames that contain ISP domain names, you can configure the device to send usernames without domain names to the servers.

If two or more ISP domains use the same HWTACACS scheme, configure the HWTACACS scheme to keep the ISP domain name in usernames for domain identification.

The device reports online user traffic statistics in accounting packets. The traffic measurement units are configurable, but they must be the same as the traffic measurement units configured on the HWTACACS accounting servers.

To set the username format and traffic statistics units for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Set the format of usernames sent to the HWTACACS servers.	user-name-format { keep-original with-domain without-domain }	By default, the ISP domain name is included in a username.
4. (Optional.) Set the data flow and packet measurement units for traffic statistics.	data-flow-format { data { byte giga-byte kilo-byte mega-byte } packet { giga-packet kilo-packet mega-packet one-packet } }*	By default, traffic is counted in bytes and packets.

Specifying the source IP address for outgoing HWTACACS packets

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. When the HWTACACS server receives a packet, it checks whether the source IP address of the packet is the IP address of a managed NAS.

- If it is the IP address of a managed NAS, the server processes the packet.
- If it is not the IP address of a managed NAS, the server drops the packet.

To communicate with the HWTACACS server, the source address of outgoing HWTACACS packets is typically the IP address of an egress interface on the NAS. However, in some situations, you must change the source IP address. For example, when VRRP is configured for stateful failover, configure the virtual IP of the uplink VRRP group as the source address.

You can specify the source IP address for outgoing HWTACACS packets in HWTACACS scheme view or in system view.

- The IP address specified in HWTACACS scheme view applies to one HWTACACS scheme.
- The IP address specified in system view applies to all HWTACACS schemes whose servers are in a VPN or the public network.

Before sending an HWTACACS packet, the NAS selects a source IP address in the following order:

1. The source IP address specified for the HWTACACS scheme.
2. The source IP address specified in system view for the VPN or public network, depending on where the HWTACACS server resides.
3. The IP address of the outbound interface specified by the route.

To specify a source IP address for all HWTACACS schemes of a VPN or the public network:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a source IP address for outgoing HWTACACS packets.	hwtacacs nas-ip { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]	By default, the IP address of the HWTACACS packet outbound interface is used as the source IP address.

To specify a source IP address for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Specify the source IP address of outgoing HWTACACS packets.	nas-ip { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	By default, the source IP address specified by the hwtacacs nas-ip command in system view is used. If the source IP address is not specified, the IP address of the outbound interface is used.

Setting HWTACACS timers

The device uses the following timers to control communication with an HWTACACS server:

- **Server response timeout timer (response-timeout)**—Defines the HWTACACS server response timeout timer. The device starts this timer immediately after an HWTACACS authentication, authorization, or accounting request is sent. If the device does not receive a response from the server within the timer, it sets the server to blocked. Then, the device sends the request to another HWTACACS server.
- **Real-time accounting timer (realtime-accounting)**—Defines the interval at which the device sends real-time accounting packets to the HWTACACS accounting server for online users.
- **Server quiet timer (quiet)**—Defines the duration to keep an unreachable server in blocked state. If a server is not reachable, the device changes the server status to blocked, starts this timer for the server, and tries to communicate with another server in active state. After the server quiet timer expires, the device changes the status of the server back to active.

The server quiet timer setting affects the status of HWTACACS servers. If the scheme includes one primary HWTACACS server and multiple secondary HWTACACS servers, the device communicates with the HWTACACS servers based on the following rules:

- When the primary server is in active state, the device communicates with the primary server.
- If the primary server fails, the device performs the following operations:
 - Changes the server status to blocked.
 - Starts a quiet timer for the server.
 - Tries to communicate with a secondary server in active state that has the highest priority.
- If the secondary server is unreachable, the device performs the following operations:

- Changes the server status to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with the next secondary server in active state that has the highest priority.
- The search process continues until the device finds an available secondary server or has checked all secondary servers in active state. If no server is available, the device considers the authentication, authorization, or accounting attempt a failure.
- When the quiet timer of a server expires, the status of the server changes back to active. The device does not check the server again during the authentication, authorization, or accounting process.
- When you remove a server in use, communication with the server times out. The device looks for a server in active state by first checking the primary server, and then checking secondary servers in the order they are configured.
- When all servers are in blocked state, the device only tries to communicate with the primary server.
- When one or more servers are in active state, the device tries to communicate with these servers only, even if they are unavailable.
- When an HWTACACS server's status changes automatically, the device changes this server's status accordingly in all HWTACACS schemes in which this server is specified.

To set HWTACACS timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter HWTACACS scheme view.	hwtacacs scheme <i>hwtacacs-scheme-name</i>	N/A
3. Set the HWTACACS server response timeout timer.	timer response-timeout <i>seconds</i>	By default, the HWTACACS server response timeout timer is 5 seconds.
4. Set the real-time accounting interval.	timer realtime-accounting <i>minutes</i>	By default, the real-time accounting interval is 12 minutes. A short interval helps improve accounting precision but requires many system resources. When there are 1000 or more users, set a longer interval.
5. Set the server quiet timer.	timer quiet <i>minutes</i>	By default, the server quiet timer is 5 minutes.

Displaying and maintaining HWTACACS

Execute the **display** command in any view and the **reset** command in user view.

Task	Command
Display the configuration or server statistics of HWTACACS schemes.	display hwtacacs scheme [<i>hwtacacs-server-name</i>] [statistics]
Clear HWTACACS statistics.	reset hwtacacs statistics { accounting all authentication authorization }

Configuring LDAP schemes

Configuration task list

Tasks at a glance
Configuring an LDAP server:
• (Required.) Creating an LDAP server • (Required.) Configuring the IP address of the LDAP server • (Optional.) Specifying the LDAP version • (Optional.) Setting the LDAP server timeout period • (Required.) Configuring administrator attributes • (Required.) Configuring LDAP user attributes
(Optional.) Configuring an LDAP attribute map
(Required.) Creating an LDAP scheme
(Required.) Specifying the LDAP authentication server
(Optional.) Specifying the LDAP authorization server
(Optional.) Specifying an LDAP attribute map for LDAP authorization
(Optional.) Displaying and maintaining LDAP

Creating an LDAP server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an LDAP server and enter LDAP server view.	ldap server <i>server-name</i>	By default, no LDAP server exists.

Configuring the IP address of the LDAP server

Step	Command	Remarks
1. Enter system view.	System-view	N/A
2. Enter LDAP server view.	ldap server <i>server-name</i>	N/A
3. Configure the IP address of the LDAP server.	{ ip <i>ip-address</i> ipv6 <i>ipv6-address</i> } [port <i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>]	By default, an LDAP server has no IP address. You can configure either an IPv4 address or an IPv6 address for an LDAP server. The most recent configuration takes effect.

Specifying the LDAP version

Specify the LDAP version on the NAS. The device supports LDAPv2 and LDAPv3. The LDAP version specified on the device must be consistent with the version specified on the LDAP server.

To specify the LDAP version:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter LDAP server view.	ldap server <i>server-name</i>	N/A
3. Specify the LDAP version.	protocol-version { v2 v3 }	By default, LDAPv3 is used. A Microsoft LDAP server supports only LDAPv3.

Setting the LDAP server timeout period

If the device sends a bind or search request to an LDAP server without receiving the server's response within the server timeout period, the authentication or authorization request times out. Then, the device tries the backup authentication or authorization method. If no backup method is configured in the ISP domain, the device considers the authentication or authorization attempt a failure.

To set the LDAP server timeout period:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP server view.	ldap server <i>server-name</i>	N/A
3. Set the LDAP server timeout period.	server-timeout <i>time-interval</i>	By default, the LDAP server timeout period is 10 seconds.

Configuring administrator attributes

To configure the administrator DN and password for binding with the LDAP server during LDAP authentication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP server view.	ldap server <i>server-name</i>	N/A
3. Specify the administrator DN.	login-dn <i>dn-string</i>	By default, no administrator DN is specified. The administrator DN specified on the device must be the same as configured on the LDAP server.
4. Configure the administrator password.	login-password { cipher simple } <i>password</i>	By default, no administrator password is specified.

Configuring LDAP user attributes

To authenticate a user, an LDAP client must complete the following operations:

1. Establish a connection to the LDAP server.
2. Obtain the user DN from the LDAP server.
3. Use the user DN and the user's password to bind with the LDAP server.

LDAP provides a DN search mechanism for obtaining the user DN. According to the mechanism, an LDAP client sends search requests to the server based on the search policy determined by the LDAP user attributes of the LDAP client.

The LDAP user attributes include:

- Search base DN.
- Search scope.
- Username attribute.

- Username format.
- User object class.

If the LDAP server contains many directory levels, a user DN search starting from the root directory can take a long time. To improve efficiency, you can change the start point by specifying the search base DN.

To configure LDAP user attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP server view.	ldap server <i>server-name</i>	N/A
3. Specify the user search base DN.	search-base-dn <i>base-dn</i>	By default, no user search base DN is specified.
4. (Optional.) Specify the user search scope.	search-scope { all-level single-level }	By default, the user search scope is all-level .
5. (Optional.) Specify the username attribute.	user-parameters user-name-attribute { <i>name-attribute</i> cn uid }	By default, the username attribute is cn .
6. (Optional.) Specify the username format.	user-parameters user-name-format { with-domain without-domain }	By default, the username format is without-domain .
7. (Optional.) Specify the user object class.	user-parameters user-object-class <i>object-class-name</i>	By default, no user object is specified, and the default user object class on the LDAP server is used. The default user object class for this command varies by device model.

Configuring an LDAP attribute map

Configure an LDAP attribute map to define a list of LDAP-AAA attribute mapping entries. To apply the LDAP attribute map, specify the name of the LDAP attribute map in the LDAP scheme used for authorization.

The LDAP attribute map feature enables the device to convert LDAP attributes obtained from an LDAP authorization server to device-recognizable AAA attributes based on the mapping entries. Because the device ignores unrecognized LDAP attributes, configure the mapping entries to include important LDAP attributes that should not be ignored.

An LDAP attribute can be mapped only to one AAA attribute. Different LDAP attributes can be mapped to the same AAA attribute.

To configure an LDAP attribute map:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an LDAP attribute map and enter LDAP attribute map view.	ldap attribute-map <i>map-name</i>	By default, no LDAP attribute maps exist.

Step	Command	Remarks
3. Configure a mapping entry.	map ldap-attribute <i>ldap-attribute-name</i> [prefix <i>prefix-value</i> delimiter <i>delimiter-value</i>] aaa-attribute { user-group user-profile }	By default, a new LDAP attribute map does not have a mapping entry. Repeat this command to configure multiple mapping entries.

Creating an LDAP scheme

You can configure a maximum of 16 LDAP schemes. An LDAP scheme can be used by multiple ISP domains.

To create an LDAP scheme:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an LDAP scheme and enter LDAP scheme view.	ldap scheme <i>ldap-scheme-name</i>	By default, no LDAP scheme is defined.

Specifying the LDAP authentication server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP scheme view.	ldap scheme <i>ldap-scheme-name</i>	N/A
3. Specify the LDAP authentication server.	authentication-server <i>server-name</i>	By default, no LDAP authentication server is specified.

Specifying the LDAP authorization server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP scheme view.	ldap scheme <i>ldap-scheme-name</i>	N/A
3. Specify the LDAP authorization server.	authorization-server <i>server-name</i>	By default, no LDAP authorization server is specified.

Specifying an LDAP attribute map for LDAP authorization

Specify an LDAP attribute map for LDAP authorization to convert LDAP attributes obtained from the LDAP authorization server to device-recognizable AAA attributes.

You can specify only one LDAP attribute map in an LDAP scheme.

To specify an LDAP attribute map for LDAP authorization:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter LDAP scheme view.	ldap scheme <i>ldap-scheme-name</i>	N/A
3. Specify an LDAP attribute map.	attribute-map <i>map-name</i>	By default, no LDAP attribute map is specified.

Displaying and maintaining LDAP

Execute the **display** command in any view.

Task	Command
Display the configuration of LDAP schemes.	display ldap scheme [<i>scheme-name</i>]

Configuring AAA methods for ISP domains

You configure AAA methods for an ISP domain by specifying configured AAA schemes in ISP domain view. Each ISP domain has a set of system-defined AAA methods, which are local authentication, local authorization, and local accounting. If you do not configure any AAA methods for an ISP domain, the device uses the system-defined AAA methods for users in the domain.

AAA is available to login users after you enable **scheme** authentication for the users. For more information about the login authentication modes, see *Fundamentals Configuration Guide*.

Configuration prerequisites

To use local authentication for users in an ISP domain, configure local user accounts on the device first. See ["Configuring local user attributes."](#)

To use remote authentication, authorization, and accounting, create the required RADIUS, HWTACACS, or LDAP schemes. For more information about the scheme configuration, see ["Configuring RADIUS schemes,"](#) ["Configuring HWTACACS schemes,"](#) and ["Configuring LDAP schemes."](#)

Creating an ISP domain

In a networking scenario with multiple ISPs, the device can connect to users of different ISPs. These users can have different user attributes, such as different username and password structures, different service types, and different rights. To manage users of different ISPs, configure ISP domains, and configure AAA methods and domain attributes for each ISP domain as needed.

The device supports a maximum of 16 ISP domains, including the system-defined ISP domain **system**. You can specify one of the ISP domains as the default domain.

On the device, each user belongs to an ISP domain. If a user does not provide an ISP domain name at login, the device considers the user belongs to the default ISP domain.

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users who are assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

NOTE:

Support for the authentication domain configuration depends on the access module. You can specify an authentication domain for 802.1X, portal, or MAC authentication.

When you configure an ISP domain, follow these restrictions and guidelines:

- An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- You can modify the settings of the system-defined ISP domain **system**, but you cannot delete the domain.
- An ISP domain cannot be deleted when it accommodates users who are assigned to nonexistent domains. Before you use the **undo domain** command, restore the default setting of the ISP domain by using the **undo domain if-unknown** command.

To create an ISP domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an ISP domain and enter ISP domain view.	domain <i>isp-name</i>	By default, the device has a system-defined ISP domain system .
3. Return to system view.	quit	N/A
4. (Optional.) Specify the default ISP domain.	domain default enable <i>isp-name</i>	By default, the default ISP domain is the system-defined ISP domain system .
5. (Optional.) Specify the ISP domain to accommodate users who are assigned to nonexistent domains.	domain if-unknown <i>isp-domain-name</i>	By default, no ISP domain is specified to accommodate users who are assigned to nonexistent domains.

Configuring ISP domain attributes

In an ISP domain, you can configure the following attributes:

- **Domain status**—By placing the ISP domain in active or blocked state, you allow or deny network service requests from users in the domain.
- **Authorization attributes**—The device assigns the authorization attributes in the ISP domain to the authenticated users who do not receive these attributes from the server. However, if the idle cut attribute is configured in the ISP domain, the device assigns the attribute to the authenticated users. If no idle cut attribute is configured in the ISP domain, the device uses the idle cut attribute assigned by the server. The device supports the following authorization attributes:
 - **Authorization ACL**—The device restricts authenticated users to access only the network resources permitted by the ACL. For portal users, the authorization ACL can be configured in a preauthentication domain to authorize access to network resources before users pass authentication.
 - **Authorization CAR action**—The attribute controls the traffic flow of authenticated users. For portal users, the authorization CAR action can be configured in a preauthentication domain to control traffic flow before users pass authentication.
 - **Idle cut**—It enables the device to check the traffic of each online user in the domain at the idle timeout interval. The device logs out any users in the domain whose total traffic in the idle timeout period is less than the specified minimum traffic.
 - **IPv4 address pool**—The device assigns IPv4 addresses from the pool to authenticated IPoE, portal, or PPP users in the domain.
 - **Default authorization user profile**—When a user passes authentication, it typically obtains an authorization user profile from the local or remote server. If the user does not obtain any user profile, the device authorizes the default user profile of the ISP domain to the user. The device will restrict the user's behavior based on the profile. For portal users, the authorization user profile can be configured in a preauthentication domain to restrict user behaviors before users pass authentication.

- **Authorization session group profile**—The device restricts authenticated users' behaviors based on the settings in the authorization session group profile. For portal users, the authorization session group profile can be configured in a preauthentication domain to restrict user behaviors before users pass authentication.
- **Authorization IPv6 address prefix**—The device authorizes the IPv6 address prefix to authenticated IPoE or PPP users in the domain.
- **IPv6 address pool**—The device assigns IPv6 addresses from the pool to authenticated IPoE, portal, or PPP users in the domain.
- **DNS server address**—The attribute specifies the DNS server that offers DNS services to the authenticated PPP users in the domain.
- **Redirect URL**—The device redirects PPP users in the domain to the URL after they pass authentication.
- **Authorization user group**—Authenticated users in the domain obtain all attributes of the user group.
- **Authorization VPN instance**—The device allows authenticated PPP and IPoE users in the domain to access network resources in the authorization VPN.
- **Maximum number of multicast groups**—The attribute restricts the maximum number of multicast groups that an authenticated IPoE, portal, or PPP user can join concurrently.
- **User online duration including idle cut period**—If a user goes offline due to connection failure or malfunction, its online duration sent to the server includes the idle cut period or user online detection period. The online duration that is generated on the server is longer than the actual online duration of the user. The user online detection period is supported only by portal authentication.
- **ITA policy**—The attribute allows the device to perform accounting at different charge rates for user data based on destination addresses. The ITA policy assigned from an AAA server takes precedence over the ITA policy in an ISP domain.

An ISP domain attribute applies to all users in the domain.

To configure ISP domain attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter ISP domain view.	domain <i>isp-name</i>	N/A
3. Place the ISP domain in active or blocked state.	state { active block }	By default, an ISP domain is in active state, and users in the domain can request network services.

Step	Command	Remarks
4. Configure authorization attributes for authenticated users in the ISP domain.	authorization-attribute { acl <i>acl-number</i> car inbound cir <i>committed-information-rate</i> [pir <i>peak-information-rate</i>] outbound cir <i>committed-information-rate</i> [pir <i>peak-information-rate</i>] idle-cut <i>minute</i> [<i>flow</i>] igmp max-access-number <i>number</i> ip-pool <i>pool-name</i> ipv6-pool <i>ipv6-pool-name</i> ipv6-prefix <i>ipv6-prefix</i> <i>prefix-length</i> mld max-access-number <i>number</i> { primary-dns secondary-dns } { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } session-group-profile <i>session-group-profile-name</i> url <i>url-string</i> user-group <i>user-group-name</i> user-profile <i>profile-name</i> vpn-instance <i>vpn-instance-name</i> }	By default, the authorization attributes are not configured and the idle cut function is disabled.
5. Configure the device to include the idle cut period or user online detection period in the user online duration to be sent to the server.	session-time include-idle-time	By default, the user online duration sent to the server does not include the idle cut period or user online detection period.
6. Specify the user address type in the ISP domain.	user-address-type { ds-lite ipv6 nat64 private-ds private-ipv4 public-ds public-ipv4 }	By default, no user address type is specified.
7. Specify the service type for users in the ISP domain.	service-type { hsi stb voip }	By default, the service type is hsi .
8. Specify the ITA policy for users in the ISP domain.	ita-policy <i>policy-name</i>	By default, no ITA policy is specified.

Configuring authentication methods for an ISP domain

Configuration prerequisites

Before configuring authentication methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an authentication method for each access type and service type.
2. Determine whether to configure the default authentication method for all access types or service types. The default authentication method applies to all access users. However, the method has a lower priority than the authentication method that is specified for an access type or service type.

Configuration guidelines

When configuring authentication methods, follow these guidelines:

- If the authentication method uses a RADIUS scheme and the authorization method does not use a RADIUS scheme, AAA accepts only the authentication result from the RADIUS server. The Access-Accept message from the RADIUS server also includes the authorization information, but the device ignores the information.
- If an HWTACACS scheme is specified, the device uses the entered username for role authentication. If a RADIUS scheme is specified, the device uses the username **\$enabn\$** on

the RADIUS server for role authentication. The variable *n* represents a user role level. For more information about user role authentication, see *Fundamentals Configuration Guide*.

Configuration procedure

To configure authentication methods for an ISP domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter ISP domain view.	domain <i>isp-name</i>	N/A
3. Specify the default authentication method for all types of users.	authentication default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default authentication method is local . The none keyword is not supported in FIPS mode.
4. Specify the authentication method for ADVPN users.	authentication advpn { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authentication method is used for ADVPN users. The none keyword is not supported in FIPS mode.
5. Specify the authentication method for IPoE users.	authentication ipoe { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authentication method is used for IPoE users. The none keyword is not supported in FIPS mode.
6. Specify the authentication method for LAN users.	authentication lan-access { ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authentication method is used for LAN users. The none keyword is not supported in FIPS mode.
7. Specify the authentication method for login users.	authentication login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default authentication method is used for login users. The none keyword is not supported in FIPS mode.
8. Specify the authentication method for portal users.	authentication portal { ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authentication method is used for portal users. The none keyword is not supported in FIPS mode.
9. Specify the authentication method for PPP users.	authentication ppp { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default authentication method is used for PPP users. The none keyword is not supported in FIPS mode.

Step	Command	Remarks
10. Specify the authentication method for SSL VPN users.	authentication sslvpn { ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authentication method is used for SSL VPN users. The none keyword is not supported in FIPS mode.
11. Specify the authentication method for obtaining a temporary user role.	authentication super { hwtacacs-scheme <i>hwtacacs-scheme-name</i> radius-scheme <i>radius-scheme-name</i> } *	By default, the default authentication method is used for obtaining a temporary user role.

Configuring authorization methods for an ISP domain

Configuration prerequisites

Before configuring authorization methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an authorization scheme for each access type and service type.
2. Determine whether to configure the default authorization method for all access types or service types. The default authorization method applies to all access users. However, the method has a lower priority than the authorization method that is specified for an access type or service type.

Configuration guidelines

When configuring authorization methods, follow these guidelines:

- The device supports HWTACACS authorization but not LDAP authorization.
- To use a RADIUS scheme as the authorization method, specify the name of the RADIUS scheme that is configured as the authentication method for the ISP domain. If an invalid RADIUS scheme is specified as the authorization method, RADIUS authentication and authorization fail.

Configuration procedure

To configure authorization methods for an ISP domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter ISP domain view.	domain <i>isp-name</i>	N/A
3. Specify the default authorization method for all types of users.	authorization default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the authorization method is local . The none keyword is not supported in FIPS mode.
4. Specify the authorization method for ADVPN users.	authorization advpn { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authorization method is used for ADVPN users. The none keyword is not supported in FIPS mode.

Step	Command	Remarks
5. Specify the command authorization method.	authorization command { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local [none] local [none] none }	By default, the default authorization method is used for command authorization. The none keyword is not supported in FIPS mode.
6. Specify the authorization method for IPoE users.	authorization ipoe { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authorization method is used for IPoE users. The none keyword is not supported in FIPS mode.
7. Specify the authorization method for LAN users.	authorization lan-access { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authorization method is used for LAN users. The none keyword is not supported in FIPS mode.
8. Specify the authorization method for login users.	authorization login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default authorization method is used for login users. The none keyword is not supported in FIPS mode.
9. Specify the authorization method for portal users.	authorization portal { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authorization method is used for portal users. The none keyword is not supported in FIPS mode.
10. Specify the authorization method for PPP users.	authorization ppp { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default authorization method is used for PPP users. The none keyword is not supported in FIPS mode.
11. Specify the authorization method for SSL VPN users.	authorization sslvpn { ldap-scheme <i>ldap-scheme-name</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default authorization method is used for SSL VPN users. The none keyword is not supported in FIPS mode.

Configuring accounting methods for an ISP domain

Configuration prerequisites

Before configuring accounting methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an accounting method for each access type and service type.
2. Determine whether to configure the default accounting method for all access types or service types. The default accounting method applies to all access users. However, the method has a lower priority than the accounting method that is specified for an access type or service type.

Configuration guidelines

When configuring accounting methods, follow these guidelines:

- FTP, SFTP, and SCP users do not support accounting.
- Local accounting does not provide statistics for charging. It only counts and controls the number of concurrent users who use the same local user account. The threshold is configured by using the **access-limit** command.

Configuration procedure

To configure accounting methods for an ISP domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter ISP domain view.	domain <i>isp-name</i>	N/A
3. Specify the default accounting method for all types of users.	accounting default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the accounting method is local . The none keyword is not supported in FIPS mode.
4. Specify the accounting method for ADVPN users.	accounting advpn { local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default accounting method is used for ADVPN users. The none keyword is not supported in FIPS mode.
5. Specify the command accounting method.	accounting command hwtacacs-scheme <i>hwtacacs-scheme-name</i>	By default, the default accounting method is used for command accounting.
6. Specify the accounting method for IPoE users.	accounting ipoe { broadcast radius-scheme <i>radius-scheme-name1</i> radius-scheme <i>radius-scheme-name2</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default accounting method is used for IPoE users. The none keyword is not supported in FIPS mode.
7. Specify the accounting method for LAN users.	accounting lan-access { broadcast radius-scheme <i>radius-scheme-name1</i> radius-scheme <i>radius-scheme-name2</i> [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [local] [none] }	By default, the default accounting method is used for LAN users. The none keyword is not supported in FIPS mode.
8. Specify the accounting method for login users.	accounting login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [radius-scheme <i>radius-scheme-name</i>] [local] [none] local [none] none radius-scheme <i>radius-scheme-name</i> [hwtacacs-scheme <i>hwtacacs-scheme-name</i>] [local] [none] }	By default, the default accounting method is used for login users. The none keyword is not supported in FIPS mode.

Step	Command	Remarks
9. Specify the accounting method for portal users.	accounting portal { broadcast radius-scheme radius-scheme-name1 radius-scheme radius-scheme-name2 [local] [none] local [none] none radius-scheme radius-scheme-name [local] [none] }	By default, the default accounting method is used for portal users. The none keyword is not supported in FIPS mode.
10. Specify the accounting method for PPP users.	accounting ppp { broadcast radius-scheme radius-scheme-name1 radius-scheme radius-scheme-name2 [hwtacacs-scheme hwtacacs-scheme-name] [local] [none] hwtacacs-scheme hwtacacs-scheme-name [radius-scheme radius-scheme-name] [local] [none] local [none] none radius-scheme radius-scheme-name [hwtacacs-scheme hwtacacs-scheme-name] [local] [none] }	By default, the default accounting method is used for PPP users. The none keyword is not supported in FIPS mode.
11. Specify the accounting method for SSL VPN users.	accounting sslvpn { local [none] none radius-scheme radius-scheme-name [local] [none] }	By default, the default accounting method is used for SSL VPN users. The none keyword is not supported in FIPS mode.
12. Configure access control for users who encounter accounting-start failures.	accounting start-fail { offline online }	By default, the device does not perform actions on users who encounter account-start failures.
13. Configure access control for users who have failed all their accounting-update attempts.	accounting update-fail { [max-times times] offline online }	By default, the device does not perform actions on users who have failed all their accounting-update attempts.
14. Configure access control for users who have used up their data quotas.	accounting quota-out { offline online }	By default, the device logs off users who have used up their data quotas.

Enabling the session-control feature

A RADIUS server running on IMC can use session-control packets to inform disconnect or dynamic authorization change requests. This task enables the device to receive RADIUS session-control packets on UDP port 1812.

To enable the session-control feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the session-control feature.	radius session-control enable	By default, the session-control feature is disabled.

Configuring the RADIUS DAE server feature

Dynamic Authorization Extensions (DAE) to RADIUS, defined in RFC 5176, can log off online users or change their authorization information. DAE uses the client/server model.

In a RADIUS network, the RADIUS server typically acts as the DAE client and the NAS acts as the DAE server.

When the RADIUS DAE server feature is enabled, the NAS performs the following operations:

1. Listens to the default or specified UDP port to receive DAE requests.
2. Logs off online users who match the criteria in the requests, or changes their authorization information.
3. Sends DAE responses to the DAE client.

DAE defines the following types of packets:

- **Disconnect Messages (DMs)**—The DAE client sends DM requests to the DAE server to log off specific online users.
- **Change of Authorization Messages (CoA Messages)**—The DAE client sends CoA requests to the DAE server to change the authorization information of specific online users.

To configure the RADIUS DAE server feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the RADIUS DAE server feature and enter RADIUS DAE server view.	radius dynamic-author server	By default, the RADIUS DAE server feature is disabled.
3. Specify a RADIUS DAE client.	client { ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [key { cipher simple } string vpn-instance <i>vpn-instance-name</i>] *	By default, no RADIUS DAE client is specified.
4. Specify the RADIUS DAE server port.	port <i>port-number</i>	By default, the RADIUS DAE server port is 3799.

Changing the DSCP priority for RADIUS packets

The DSCP priority in the ToS field determines the transmission priority of RADIUS packets. A larger value represents a higher priority.

To change the DSCP priority for RADIUS packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Change the DSCP priority for RADIUS packets.	radius [ipv6] dscp <i>dscp-value</i>	By default, the DSCP priority is 0 for RADIUS packets.

Setting the maximum number of concurrent login users

Perform this task to set the maximum number of concurrent users who can log on to the device through a specific protocol, regardless of their authentication methods. The authentication methods include no authentication, local authentication, and remote authentication.

To set the maximum number of concurrent login users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the maximum number of concurrent login users.	- In non-FIPS mode: aaa session-limit { ftp http https ssh telnet } max-sessions - In FIPS mode: aaa session-limit { https ssh } max-sessions	By default, the maximum number of concurrent login users is 32 for FTP, SSH, and Telnet users, and 64 for HTTP and HTTPS users.

Configuring and applying an ITA policy

Intelligent Target Accounting (ITA) provides a flexible accounting solution for users who request services of different charge rates. ITA separates accounting statistics at different levels.

ITA services are supported only for portal, IPoE, and PPP users.

You must deploy an ITA policy to implement ITA services.

To deploy an ITA policy, perform the following tasks:

1. Configure a QoS policy to remark traffic destined for different IP addresses or subnets to different levels. For more information about QoS, see *ACL and QoS Configuration Guide*.
2. Configure a user profile, and apply the QoS policy to the user profile. For more information about user profiles, see "Configure user profiles."
3. Authorize the user profile to authenticated users. The following methods are available:
 - Specify a remote server or configure the device to assign the user profile.
 - Specify the user profile in the authentication domain.
4. Configure an ITA policy, which includes the accounting methods, traffic levels, and access control for users who have used up their ITA data quotas.
5. Apply the ITA policy to authenticated users. The following methods are available:
 - Specify a RADIUS server to assign the ITA policy.
 - Specify the ITA policy in the authentication domain.

You can configure accounting methods for an ITA policy. ITA accounting is separated from accounting of other services. However, you can configure the device to include the amount of ITA traffic in the overall traffic statistics sent to the accounting server.

To configure and apply an ITA policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Create an ITA policy and enter ITA policy view.	ita policy <i>policy-name</i>	By default, no ITA policy exists.
3. Specify the accounting method in the ITA policy.	accounting-method { none radius-scheme <i>radius-scheme-name</i> [none] }	By default, the accounting method is none .
4. Specify a traffic level for ITA accounting.	accounting-level <i>level</i> { ipv4 ipv6 }	By default, no traffic level is specified for ITA accounting.
5. (Optional.) Enable accounting merge.	accounting-merge enable	By default, accounting merge is disabled.
6. (Optional.) Configure access control for users who have used up their ITA data quotas.	traffic-quota-out { offline online }	By default, the users cannot access the authorized IP subnets after they use up their ITA data quotas.
7. (Optional.) Exclude the amount of ITA traffic from the overall traffic statistics sent to the accounting server.	traffic-separate enable	By default, the amount of ITA traffic is included in the overall traffic statistics sent to the accounting server.

Configuring a NAS-ID profile

By default, the device sends its device name in the NAS-Identifier attribute of all RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to portal- or port security-enabled interfaces. For more information, see "Configuring portal" and "[Configuring port security](#)."

A NAS-ID can be bound with more than one VLAN, but a VLAN can be bound with only one NAS-ID.

To configure a NAS-ID profile:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a NAS-ID profile and enter NAS-ID profile view.	aaa nas-id profile <i>profile-name</i>	By default, no NAS-ID profile exists.
3. Configure a NAS-ID and VLAN binding in the profile.	nas-id <i>nas-identifier</i> bind vlan <i>vlan-id</i>	By default, no NAS-ID and VLAN binding exists.

Configuring the Acct-Session-Id format

The device supports the following Acct-Session-Id formats:

- **Common**—The Acct-Session-Id is a string of 38 characters. The string contains the session-id-prefix, date and time, serial number, LIP address of the access node, device ID, and the process job ID.
- **Simplified**—The Acct-Session-Id is a string of 16 characters. The string contains the session-id-prefix, month, serial number, LIP address of the access node, device ID, and the process job ID.

Configure the Acct-Session-Id format depending on the server model. For example, the AsialInfo server supports only the 16-character Acct-Session-Id, so you must specify the simplified format on the device to work with the server.

To configure the Acct-Session-Id format:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the Acct-Session-Id format.	aaa session-id mode { common simplified }	By default, the common format is used.

Displaying and maintaining AAA

Execute **display** commands in any view.

Task	Command
Display the configuration of ISP domains.	display domain [<i>isp-name</i>]

AAA configuration examples

Authentication and authorization for SSH users by a RADIUS server

Network requirements

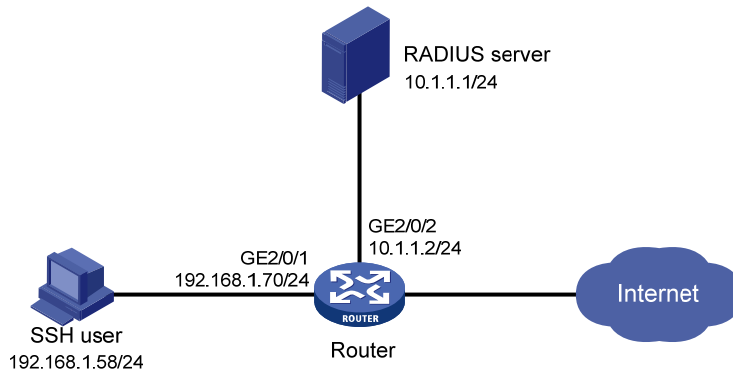
As shown in [Figure 12](#), configure the router to meet the following requirements:

- Use the RADIUS server for SSH user authentication and authorization.
- Include domain names in the usernames sent to the RADIUS server.
- Assign the default user role **network-operator** to SSH users after they pass authentication.

The RADIUS server runs on IMC. Add an account with the username **hello@bbb** on the RADIUS server.

The RADIUS server and the router use **expert** as the shared key for secure RADIUS communication. The ports for authentication and accounting are **1812** and **1813**, respectively.

Figure 12 Network diagram



Configuration procedure

1. Configure the RADIUS server on IMC 5.0:

NOTE:

In this example, the RADIUS server runs on IMC PLAT 5.0 (E0101) and IMC UAM 5.0 (E0101).

Add the router to the IMC Platform as an access device.

Log in to IMC, click the **Service** tab, and select **User Access Manager > Access Device Management > Access Device** from the navigation tree. Then, click **Add** to configure an access device as follows:

- a. Set the shared key for secure RADIUS communication to **expert**.
- b. Set the ports for authentication and accounting to 1812 and 1813, respectively.
- c. Select the service type **Device Management Service**.
- d. Select the access device type **HPE**.
- e. Select the access device from the device list or manually add the access device (with the IP address 10.1.1.2).
- f. Leave the default settings for other parameters and click **OK**.

The IP address of the access device specified here must be the same as the source IP address of the RADIUS packets sent from the router. The source IP address is chosen in the following order on the router:

- o IP address specified by the **nas-ip** command.
- o IP address specified by the **radius nas-ip** command.
- o IP address of the outbound interface (the default).

Figure 13 Adding the router as an access device

Service >> User Access Manager >> Access Device >> Add Access Device

Access Configuration

* Shared Key	expert	* Authentication Port	1812
* Accounting Port	1813	Service Type	Device Management S
Access Device Type	HPE	RADIUS Accounting	Fully Supported
Service Group	Ungrouped	Access Area	--

Device List

Select Add Manually Clear All Click OK to save your change.

Total Items: 1.

Device Name	Device IP	Device Model	Delete
	10.1.1.2		✖

OK Cancel

Add an account for device management.

Click the **User** tab, and select **Access User View > Device Mgmt User** from the navigation tree. Then, click **Add** to configure a device management account as follows:

- Enter the account name **hello@bbb** and specify the password.
- Select the service type **SSH**.
- Specify 10.1.1.0 to 10.1.1.255 as the IP address range of the hosts to be managed.
- Click **OK**.

NOTE:

The IP address range must contain the IP address of the router.

Figure 14 Adding an account for device management

User >> Device Management User >> Add Device Management User

Add Device Management User

Basic Information of Device Management User

* Account Name ?

* User Password

* Confirm Password

Service Type ▼

EXEC Priority ?

Bound User IP List

No match found.

☐	Start IP	End IP	Delete

IP Address List of Managed Devices

Total Items: 1.

☐	Start IP	End IP	Delete
☐	10.1.1.0	10.1.1.255	✗

2. Configure the router:

Configure the IP address of interface GigabitEthernet 2/0/1, through which the SSH user accesses the router.

```
<Router> system-view
```

```
[Router] interface gigabitethernet 2/0/1
```

```
[Router-GigabitEthernet2/0/1] ip address 192.168.1.70 255.255.255.0
```

```
[Router-GigabitEthernet2/0/1] quit
```

Configure the IP address of interface GigabitEthernet 2/0/2, through which the router communicates with the server.

```
[Router] interface gigabitethernet 2/0/2
```

```
[Router-GigabitEthernet2/0/2] ip address 10.1.1.2 255.255.255.0
```

```
[Router-GigabitEthernet2/0/2] quit
```

Create local RSA and DSA key pairs.

```
[Router] public-key local create rsa
```

```
[Router] public-key local create dsa
```

Enable the SSH service.

```
[Router] ssh server enable
```

Enable scheme authentication for user lines VTY 0 through VTY 63.

```
[Router] line vty 0 63
```

```
[Router-line-vty0-63] authentication-mode scheme
```

```
[Router-line-vty0-63] quit
```

Enable the default user role feature to assign authenticated SSH users the default user role **network-operator**.

```
[Router] role default-role enable
```

```

# Create a RADIUS scheme.
[Router] radius scheme rad

# Specify the primary authentication server.
[Router-radius-rad] primary authentication 10.1.1.1 1812

# Set the shared key for secure communication with the server to expert in plain text.
[Router-radius-rad] key authentication simple expert

# Include domain names in the usernames sent to the RADIUS server.
[Router-radius-rad] user-name-format with-domain
[Router-radius-rad] quit

# Create ISP domain bbb and configure authentication, authorization, and accounting methods
for login users. Because RADIUS user authorization information is piggybacked in
authentication responses, the authentication and authorization methods must use the same
RADIUS scheme.
[Router] domain bbb
[Router-isp-bbb] authentication login radius-scheme rad
[Router-isp-bbb] authorization login radius-scheme rad
[Router-isp-bbb] accounting login none
[Router-isp-bbb] quit

```

Verifying the configuration

```

# Initiate an SSH connection to the router, and enter the username hello@bbb and the correct
password. The user logs in to the router. (Details not shown.)

# Verify that the user can use the commands permitted by the network-operator user role. (Details
not shown.)

```

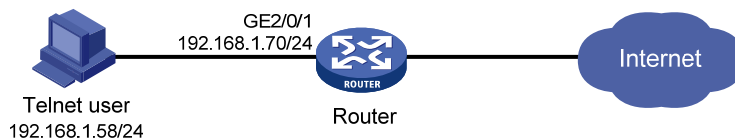
Local authentication and authorization for SSH users

Network requirements

As shown in [Figure 15](#), configure the router to meet the following requirements:

- Perform local authentication and authorization for SSH users.
- Assign the **network-admin** user role to SSH users after they pass authentication.

Figure 15 Network diagram



Configuration procedure

```

# Configure the IP address of interface GigabitEthernet 2/0/1, through which the SSH user accesses
the router.
<Router> system-view
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/0/1] quit

# Create local RSA and DSA key pairs.
[Router] public-key local create rsa
[Router] public-key local create dsa

```

```

# Enable the SSH service.
[Router] ssh server enable

# Enable scheme authentication for user lines VTY 0 through VTY 63.
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit

# Create a device management user.
[Router] local-user ssh class manage

# Assign the SSH service for the local user.
[Router-luser-manage-ssh] service-type ssh

# Set a password for the local user to 123456TESTplat&! in plain text. In FIPS mode, you must set
the password in interactive mode.
[Router-luser-manage-ssh] password simple 123456TESTplat&!

# Specify the user role for the user as network-admin.
[Router-luser-manage-ssh] authorization-attribute user-role network-admin
[Router-luser-manage-ssh] quit

# Create ISP domain bbb and configure the domain to use local authentication and authorization for
login users.
[Router] domain bbb
[Router-isp-bbb] authentication login local
[Router-isp-bbb] authorization login local
[Router-isp-bbb] quit

```

Verifying the configuration

```

# Initiate an SSH connection to the router, and enter the username ssh@bbb and the correct
password. The user logs in to the router. (Details not shown.)

# Verify that the user can use the commands permitted by the network-admin user role. (Details not
shown.)

```

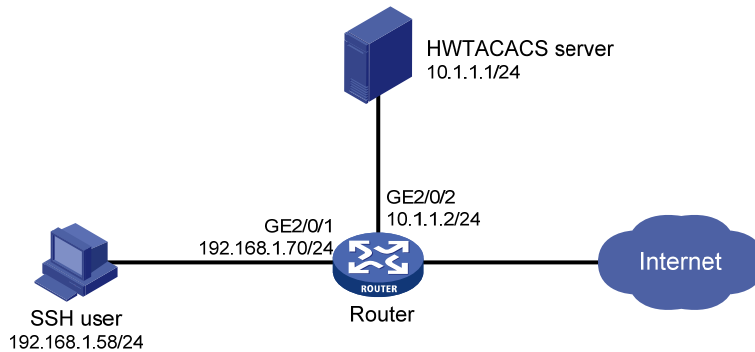
AAA for SSH users by an HWTACACS server

Network requirements

As shown in [Figure 16](#), configure the router to meet the following requirements:

- Use the HWTACACS server for SSH user authentication, authorization, and accounting.
- Assign the default user role **network-operator** to SSH users after they pass authentication.
- Exclude domain names from the usernames sent to the HWTACACS server.
- Use **expert** as the shared keys for secure HWTACACS communication.

Figure 16 Network diagram



Configuration procedure

1. Configure the HWTACACS server:
 - # Set the shared keys for secure communication with the router to **expert**. (Details not shown.)
 - # Add an account for the SSH user and specify the password. (Details not shown.)
2. Configure the router:
 - # Create an HWTACACS scheme.

```
<Router> system-view
[Router] hwtacacs scheme hwtac
```
 - # Specify the primary authentication server.

```
[Router-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```
 - # Specify the primary authorization server.

```
[Router-hwtacacs-hwtac] primary authorization 10.1.1.1 49
```
 - # Specify the primary accounting server.

```
[Router-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```
 - # Set the shared keys for secure HWTACACS communication to **expert** in plain text.

```
[Router-hwtacacs-hwtac] key authentication simple expert
[Router-hwtacacs-hwtac] key authorization simple expert
[Router-hwtacacs-hwtac] key accounting simple expert
```
 - # Exclude domain names from the usernames sent to the HWTACACS server.

```
[Router-hwtacacs-hwtac] user-name-format without-domain
[Router-hwtacacs-hwtac] quit
```
 - # Create an ISP domain and configure the domain to use the HWTACACS scheme for authentication, authorization, and accounting of login users.

```
[Router] domain bbb
[Router-isp-bbb] authentication login hwtacacs-scheme hwtac
[Router-isp-bbb] authorization login hwtacacs-scheme hwtac
[Router-isp-bbb] accounting login hwtacacs-scheme hwtac
[Router-isp-bbb] quit
```
 - # Create local RSA and DSA key pairs.

```
[Router] public-key local create rsa
[Router] public-key local create dsa
```
 - # Enable the SSH service.

```
[Router] ssh server enable
```
 - # Enable the default user role feature to assign authenticated SSH users the default user role **network-operator**.

```

[Router] role default-role enable
# Enable scheme authentication for user lines VTY 0 through VTY 63.
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
# Configure the IP address of interface GigabitEthernet 2/0/1, through which the SSH user
accesses the router.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/0/1] quit
# Configure the IP address of interface GigabitEthernet 2/0/2, through which the router is
connected to the server.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/0/2] quit

```

Verifying the configuration

Initiate an SSH connection to the router, and enter the correct username and password. The user logs in to the router. (Details not shown.)

Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Authentication for SSH users by an LDAP server

Network requirements

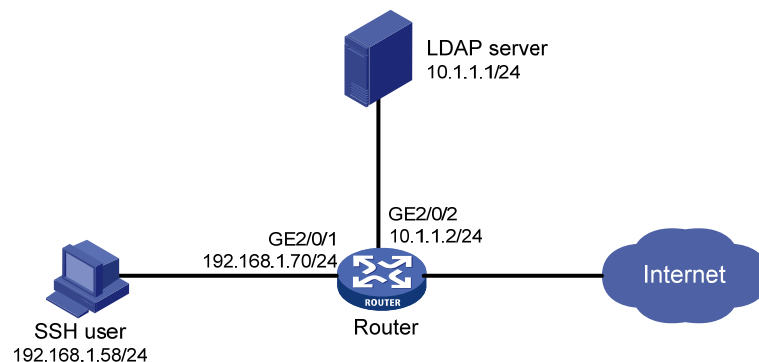
As shown in [Figure 17](#), an LDAP server is located at 10.1.1.1/24 and uses the domain name **ldap.com**.

Configure the router to meet the following requirements:

- Use the LDAP server to authenticate SSH users.
- Assign the default user role **network-operator** to SSH users after they pass authentication.

On the LDAP server, set the administrator password to **admin!123456**, add user **aaa**, and set the user's password to **ldap!123456**.

Figure 17 Network diagram



Configuration procedure

1. Configure the LDAP server:

NOTE:

In this example, the LDAP server runs Microsoft Windows 2003 Server Active Directory.

Add a user named **aaa** and set the password to **ldap!123456**.

a. On the LDAP server, select **Start > Control Panel > Administrative Tools**.

b. Double-click **Active Directory Users and Computers**.

The **Active Directory Users and Computers** window is displayed.

c. From the navigation tree, click **Users** under the **ldap.com** node.

d. Select **Action > New > User** from the menu to display the dialog box for adding a user.

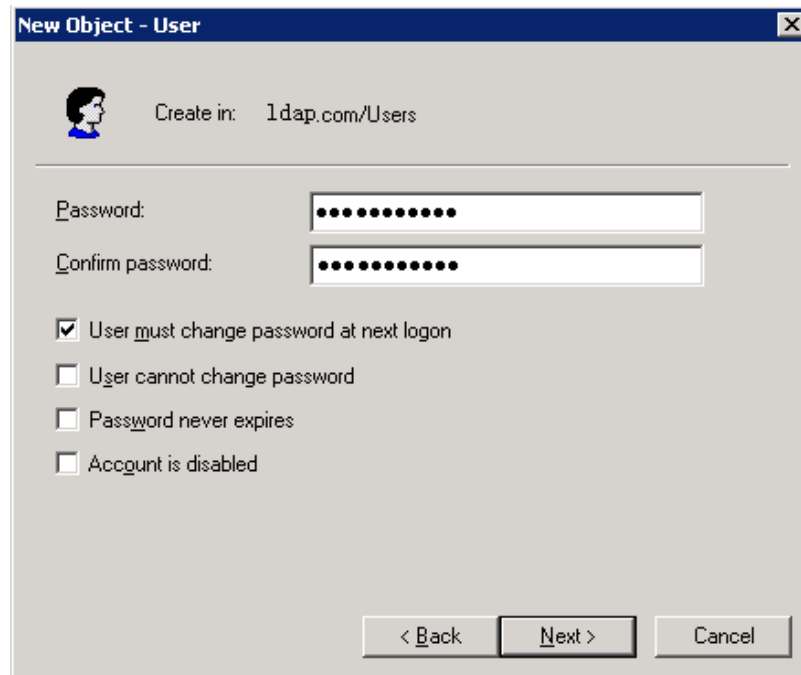
e. Enter the logon name **aaa** and click **Next**.

Figure 18 Adding user aaa

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: ldap.com/Users'. Below this, there are several input fields: 'First name' with 'aaa', 'Initials' (empty), 'Last name' (empty), 'Full name' with 'aaa', 'User logon name' with 'aaa' and a dropdown menu showing '@ldap.com', and 'User logon name (pre-Windows 2000)' with 'LDAP\' and 'aaa'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

f. In the dialog box, enter the password **ldap!123456**, select options as needed, and click **Next**.

Figure 19 Setting the user's password



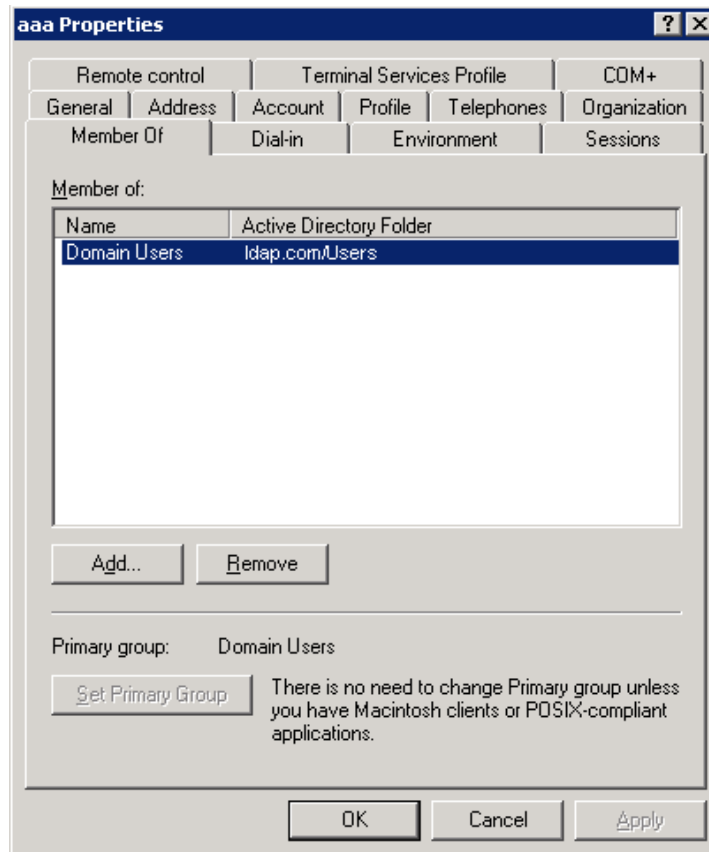
The image shows a Windows-style dialog box titled "New Object - User". At the top left is a user icon. To its right, it says "Create in: ldap.com/Users". Below this is a horizontal line. Under the line are two text input fields. The first is labeled "Password:" and the second is labeled "Confirm password:". Both fields contain ten black dots, indicating masked text. Below the input fields are four checkboxes with the following labels: "User must change password at next logon" (checked), "User cannot change password", "Password never expires", and "Account is disabled". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

g. Click **OK**.

Add user **aaa** to group **Users**.

- a. From the navigation tree, click **Users** under the **ldap.com** node.
- b. In the right pane, right-click the user **aaa** and select **Properties**.
- c. In the dialog box, click the **Member Of** tab and click **Add**.

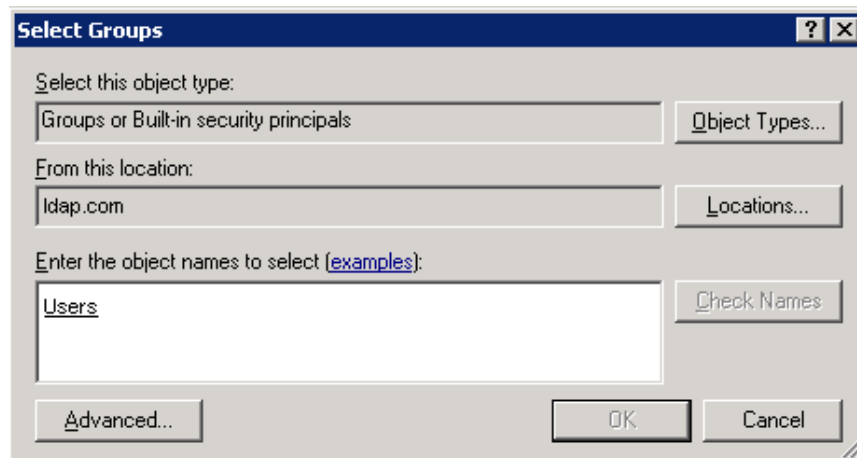
Figure 20 Modifying user properties



- d. In the **Select Groups** dialog box, enter **Users** in the **Enter the object names to select** field, and click **OK**.

User **aaa** is added to group **Users**.

Figure 21 Adding user aaa to group Users



Set the administrator password to **admin!123456**.

- a. In the right pane, right-click the user **Administrator** and select **Set Password**.
- b. In the dialog box, enter the administrator password. (Details not shown.)
2. Configure the router:

```

# Configure the IP address of interface GigabitEthernet 2/0/1, through which the SSH user
accesses the router.
<Router> system-view
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip address 192.168.1.20 24
[Router-GigabitEthernet2/0/1] quit
# Configure the IP address of interface GigabitEthernet 2/0/2, through which the router
communicates with the server.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/0/2] quit
# Create the local DSA key pair and RSA key pairs.
[Router] public-key local create dsa
[Router] public-key local create rsa
# Enable the SSH service.
[Router] ssh server enable
# Enable scheme authentication for user lines VTY 0 through VTY 63.
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
# Enable the default user role feature to assign authenticated SSH users the default user role
network-operator.
[Router] role default-role enable
# Configure an LDAP server.
[Router] ldap server ldap1
# Specify the IP address of the LDAP authentication server.
[Router-ldap-server-ldap1] ip 10.1.1.1
# Specify the administrator DN.
[Router-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com
# Specify the administrator password.
[Router-ldap-server-ldap1] login-password simple admin!123456
# Configure the base DN for user search.
[Router-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Router-ldap-server-ldap1] quit
# Create an LDAP scheme.
[Router] ldap scheme ldap1-shml
# Specify the LDAP authentication server.
[Router-ldap-ldap-shml] authentication-server ldap1
[Router-ldap-ldap1-shml] quit
# Create ISP domain bbb and configure the authentication, authorization, and accounting
methods for login users.
[Router] domain bbb
[Router-isp-bbb] authentication login ldap-scheme ldap1-shml
[Router-isp-bbb] authorization login none
[Router-isp-bbb] accounting login none
[Router-isp-bbb] quit

```

Verifying the configuration

- # Initiate an SSH connection to the router, and enter the username **aaa@bbb** and password **ldap!123456**. The user logs in to the router. (Details not shown.)
- # Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Authentication and authorization for SSL VPN users by an LDAP server

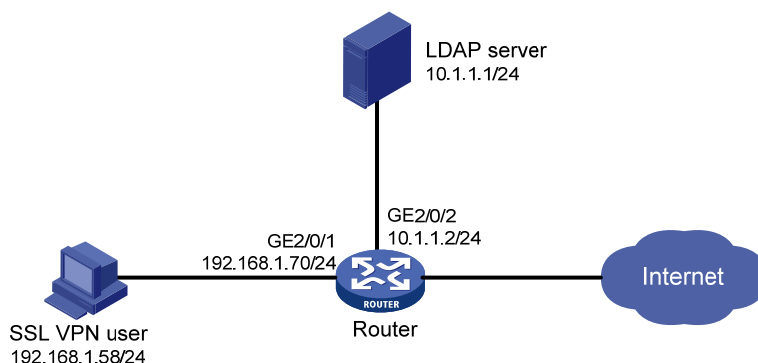
Network requirements

As shown in [Figure 22](#), configure the router to meet the following requirements:

- Use the LDAP server to perform authentication and authorization for the SSL VPN user.
- Act as an SSL VPN gateway. The gateway IP address is 192.168.1.70 and the service port number is 8080.

The LDAP server uses the domain name **ldap.com**. The server assigns an SSL VPN policy group named **pg1** to the user after authentication. The policy group defines a 120-second idle timeout for the user connections.

Figure 22 Network diagram



Configuration procedure

1. Configure the LDAP server:

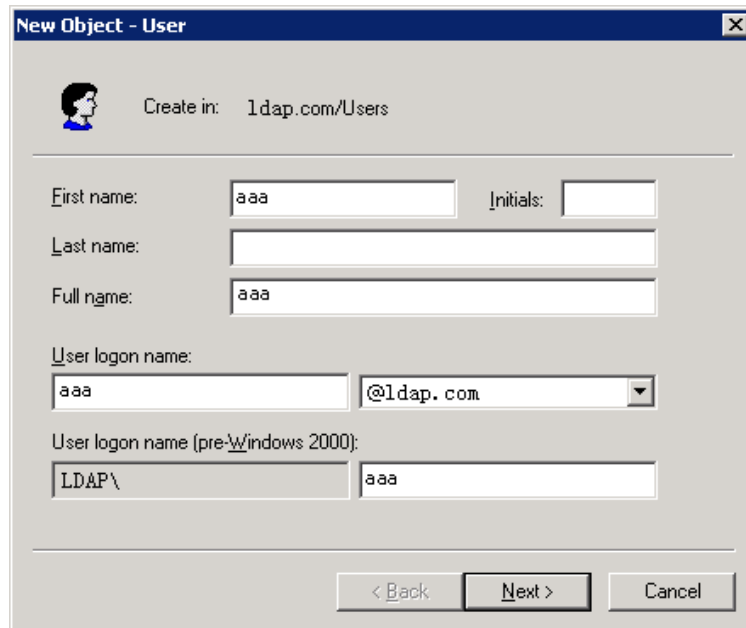
NOTE:

In this example, the LDAP server runs Microsoft Windows 2003 Server Active Directory.

Add a user named **aaa** and set the password to **ldap!123456**.

- a. On the LDAP server, select **Start > Control Panel > Administrative Tools**.
- b. Double-click **Active Directory Users and Computers**.
The **Active Directory Users and Computers** window is displayed.
- c. From the navigation tree, click **Users** under the **ldap.com** node.
- d. Select **Action > New > User** from the menu to display the dialog box for adding a user.
- e. Enter the logon name **aaa** and click **Next**.

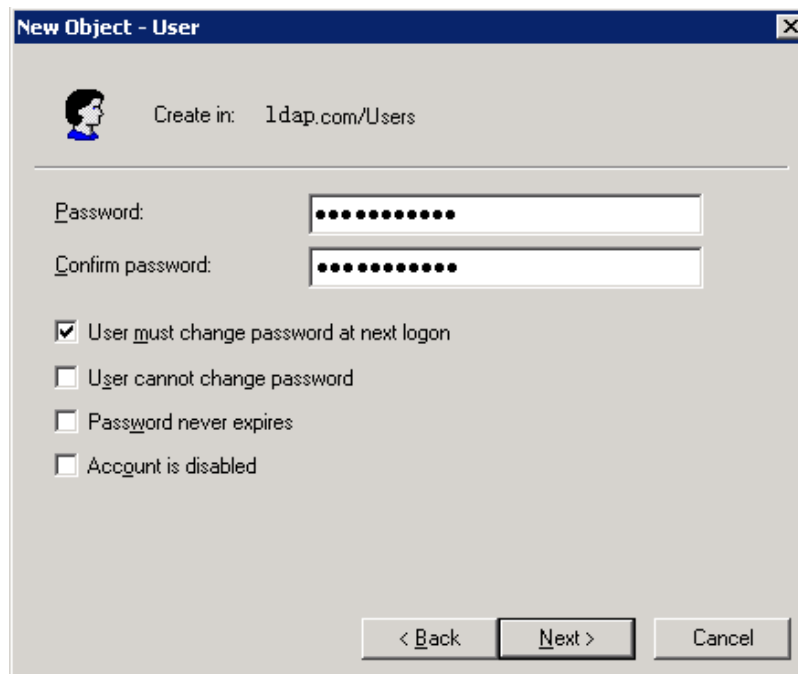
Figure 23 Adding user aaa



The 'New Object - User' dialog box is shown. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: ldap.com/Users'. The main area contains several input fields: 'First name:' with 'aaa', 'Initials:' (empty), 'Last name:' (empty), 'Full name:' with 'aaa', 'User logon name:' with 'aaa' and a dropdown menu showing '@ldap.com', and 'User logon name (pre-Windows 2000):' with 'LDAP\' and 'aaa'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- f. In the dialog box, enter the password **ldap!123456**, select options as needed, and click **Next**.

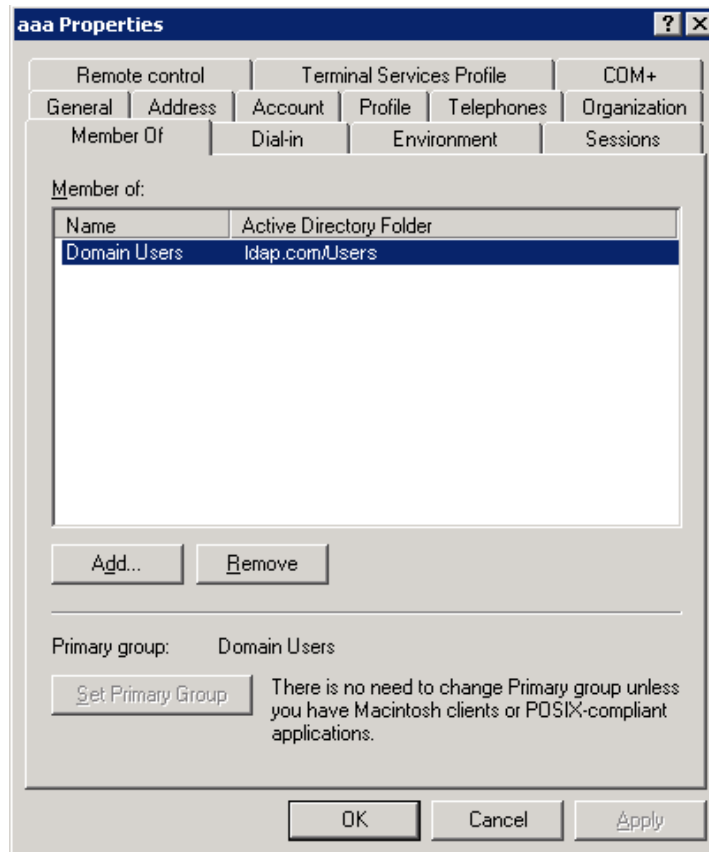
Figure 24 Setting the user's password



The 'New Object - User' dialog box is shown. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: ldap.com/Users'. The main area contains two password input fields: 'Password:' and 'Confirm password:', both filled with dots. Below these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- g. Click **OK**.
- # Add user **aaa** to group **Users**.
- a. From the navigation tree, click **Users** under the **ldap.com** node.
- b. In the right pane, right-click the user **aaa** and select **Properties**.
- c. In the dialog box, click the **Member Of** tab and click **Add**.

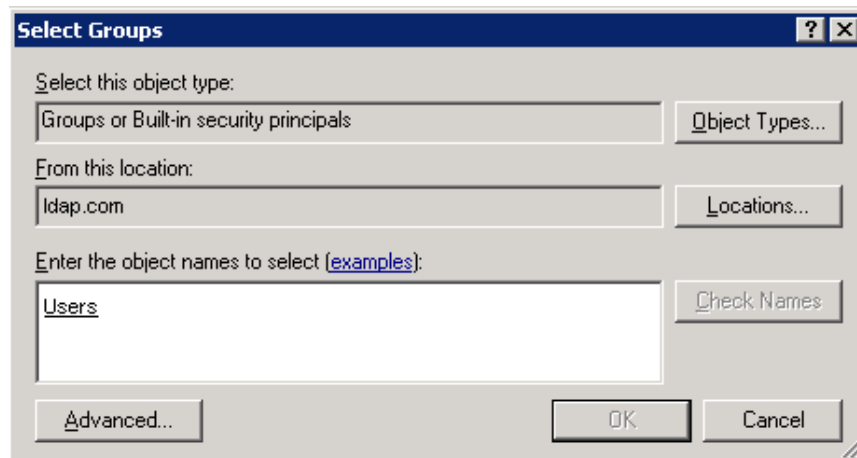
Figure 25 Modifying user properties



- d. In the **Select Groups** dialog box, enter **Users** in the **Enter the object names to select** field, and click **OK**.

User **aaa** is added to group **Users**.

Figure 26 Adding user aaa to group Users



Set the administrator password to **admin!123456**.

- a. In the right pane, right-click the user **Administrator** and select **Set Password**.
- b. In the dialog box, enter the administrator password. (Details not shown.)
2. Configure the router:

```

# Configure the IP address of interface GigabitEthernet 2/0/1, which is connected to the SSL
VPN user.
<Router> system-view
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip address 192.168.1.70 24
[Router-GigabitEthernet2/0/1] quit
# Configure the IP address of interface GigabitEthernet 2/0/2, which is connected to the LDAP
server.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] ip address 10.1.1.2 24
[Router-GigabitEthernet2/0/2] quit
# Create PKI domain sslvpn and obtain the CA and local certificates (see "Configuring PKI").
(Details not shown.)
# Create SSL server policy myssl.
[Router] ssl server-policy myssl
# Specify PKI domain sslvpn for the SSL server policy.
[Router-server-policy-myssl] pki-domain sslvpn
[Router-server-policy-myssl] quit
# Set the SSL VPN gateway name to g1.
[Router] sslvpn gateway g1
# Specify SSL server policy myssl for the SSL VPN gateway.
[Router-gateway-g1] ssl server-policy myssl
# Set the gateway IP address to 192.168.1.70 and port number to 8080.
[Router-gateway-g1] ip address 192.168.1.70 port 8080
# Enable the SSL VPN gateway.
[Router-gateway-g1] service enable
[Router-gateway-g1] quit
# Create SSL VPN context aaa.
[Router] sslvpn context aaa
# Specify gateway g1 for the SSL VPN context.
[Router-sslvpn-context-aaa] gateway g1
# Specify domain bbb for authentication, authorization, and accounting of SSL VPN users in
the context.
[Router-sslvpn-context-aaa] aaa domain bbb
# Create SSL VPN policy group pg1.
[Router-sslvpn-context-aaa] policy-group pg1
# Set the connection idle timeout timer to 120 seconds.
[Router-sslvpn-context-aaa-policy-group-pg1] timeout idle 120
[Router-sslvpn-context-aaa-policy-group-pg1] quit
# Enable the SSL VPN context.
[Router-sslvpn-context-aaa] service enable
# Configure an LDAP server.
[Router] ldap server ldap1
# Specify the IP address of the LDAP server.
[Router-ldap-server-ldap1] ip 10.1.1.1
# Specify the administrator DN.
[Router-ldap-server-ldap1] login-dn cn=admin, cn=users, dc=ldap, dc=com

```



```

# Specify the administrator password.
[Router-ldap-server-ldap1] login-password simple admin!123456
# Configure the base DN for user search.
[Router-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Router-ldap-server-ldap1] quit
# Create LDAP attribute map test.
[Router] ldap attribute-map test
# Map a partial value string of the LDAP attribute named memberof to AAA attribute named user-group.
[Router-ldap-attr-map-test] map ldap-attribute memberof prefix cn= delimiter ,
aaa-attribute user-group
[Router-ldap-attr-map-test] quit
# Create an LDAP scheme.
[Router] ldap scheme shml
# Specify the LDAP authentication and authorization servers.
[Router-ldap-shml] authentication-server ldap1
[Router-ldap-shml] authorization-server ldap1
# Specify LDAP attribute map test.
[Router-ldap-shml] attribute-map test
[Router-ldap-shml] quit
# Create ISP domain bbb, and configure the authentication, authorization, and accounting
methods for SSL VPN users.
[Router] domain bbb
[Router-isp-bbb] authentication sslvpn ldap-scheme shml
[Router-isp-bbb] authorization sslvpn ldap-scheme shml
[Router-isp-bbb] accounting sslvpn none
[Router-isp-bbb] quit
# Create user group users, and authorize SSL VPN policy group pg1 to the group.
[Router] user-group users
[Router-ugroup-users] authorization-attribute sslvpn-policy-group pg1
[Router-ugroup-users] quit

```

Verifying the configuration

```

# In the Web browser, enter https://192.168.1.70:8080 in the address bar.
# Enter username aaa@bbb and password ldap!123456. The user logs in to the website. (Details
not shown.)
# Verify that the user is assigned an SSL VPN policy group named pg1 and the user connection idle
timeout timer is 120 seconds.
[Router] display sslvpn session user aaa@bbb
User          : aaa@bbb
Context       : aaa
Policy group: pg1
Connections  : 6           User IP Address: 192.168.1.58
Last used    : 00:00:05     Created          : 18:42:10 UTC Wed 09/17/14
Idle timeout: 120 sec

```

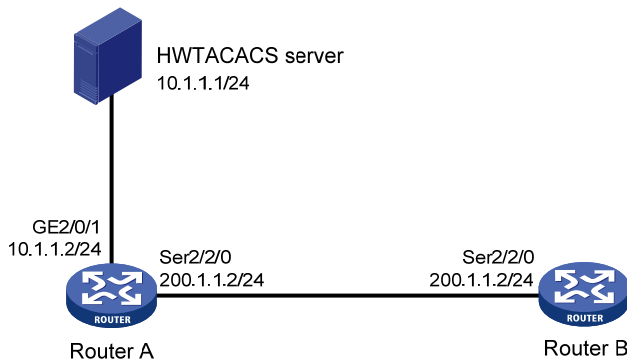
AAA for PPP users by an HWTACACS server

Network requirements

As shown in [Figure 27](#):

- Router A uses the HWTACACS server to perform PAP authentication for users from Router B.
- The HWTACACS server is also the authorization server and accounting server of Router B.
- Router B does not provide authentication, authorization, or accounting for users from Router A.

Figure 27 Network diagram



Configuration procedure

1. Configure the HWTACACS server (details not shown):
 - a. Set the shared keys for secure communication with Router A to **expert**.
 - b. Add a user account **userb** for the PPP users from Router B.
 - c. Specify the password as **passb**.
2. Configure Router A:

```
# Create an HWTACACS scheme.
<RouterA> system-view
[RouterA] hwtacacs scheme hwtac

# Configure the primary HWTACACS server at 10.1.1.1. Set the authentication, authorization,
and accounting ports to 49. Configure the router to establish only one TCP connection with the
server.
[RouterA-hwtacacs-hwtac] primary authentication 10.1.1.1 49 single-connection
[RouterA-hwtacacs-hwtac] primary authorization 10.1.1.1 49 single-connection
[RouterA-hwtacacs-hwtac] primary accounting 10.1.1.1 49 single-connection

# Set the shared keys for authentication, authorization, and accounting to expert.
[RouterA-hwtacacs-hwtac] key authentication simple expert
[RouterA-hwtacacs-hwtac] key authorization simple expert
[RouterA-hwtacacs-hwtac] key accounting simple expert

# Exclude domain names from the usernames sent to the HWTACACS server.
[RouterA-hwtacacs-hwtac] user-name-format without-domain
[RouterA-hwtacacs-hwtac] quit

# Create ISP domain bbb and configure the domain to use the HWTACACS scheme for
authentication, authorization, and accounting for PPP users.
[RouterA] domain bbb
[RouterA-isp-bbb] authentication ppp hwtacacs-scheme hwtac
[RouterA-isp-bbb] authorization ppp hwtacacs-scheme hwtac
```

```
[RouterA-isp-bbb] accounting ppp hwtacacs-scheme hwtac
[RouterA-isp-bbb] quit
# Enable PPP encapsulation on Serial 2/2/0.
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] link-protocol ppp
# Configure interface Serial 2/2/0 to authenticate the peer by using PAP in authentication
domain bbb.
[RouterA-Serial2/2/0] ppp authentication-mode pap domain bbb
# Configure the IP address of interface Serial 2/2/0.
[RouterA-Serial2/2/0] ip address 200.1.1.1 24
[RouterA-Serial2/2/0] quit
```

3. Configure Router B:

```
# Enable PPP encapsulation on Serial 2/2/0.
<RouterB> system-view
[RouterB] interface serial 2/2/0
[RouterB-Serial2/2/0] link-protocol ppp
# Configure the local username and password for PAP authentication to userb and plaintext
passb, respectively.
[RouterB-Serial2/2/0] ppp pap local-user userb password simple passb
# Configure the IP address of interface Serial 2/2/0.
[RouterB-Serial2/2/0] ip address 200.1.1.2 24
[RouterB-Serial2/2/0] quit
```

Verifying the configuration

Use the **display interface serial** command to display information for Serial 2/2/0. The PPP link is established if the output contains the following information:

- Both the physical layer and link layer are up.
- LCP and IPCP have entered the Opened state.

Router A and Router B can ping each other.

Troubleshooting RADIUS

RADIUS authentication failure

Symptom

User authentication always fails.

Analysis

Possible reasons include:

- A communication failure exists between the NAS and the RADIUS server.
- The username is not in the *userid@isp-name* format, or the ISP domain is not correctly configured on the NAS.
- The user is not configured on the RADIUS server.
- The password entered by the user is incorrect.
- The RADIUS server and the NAS are configured with different shared keys.

Solution

To resolve the problem:

1. Check the following items:
 - The NAS and the RADIUS server can ping each other.
 - The username is in the *userid@isp-name* format and the ISP domain is correctly configured on the NAS.
 - The user is configured on the RADIUS server.
 - The correct password is entered.
 - The same shared key is configured on both the RADIUS server and the NAS.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

RADIUS packet delivery failure

Symptom

RADIUS packets cannot reach the RADIUS server.

Analysis

Possible reasons include:

- A communication failure exists between the NAS and the RADIUS server.
- The NAS is not configured with the IP address of the RADIUS server.
- The authentication and accounting UDP ports configured on the NAS are incorrect.
- The RADIUS server's authentication and accounting port numbers are being used by other applications.

Solution

To resolve the problem:

1. Check the following items:
 - The link between the NAS and the RADIUS server work well at both the physical and data link layers.
 - The IP address of the RADIUS server is correctly configured on the NAS.
 - The authentication and accounting UDP port numbers configured on the NAS are the same as those of the RADIUS server.
 - The RADIUS server's authentication and accounting port numbers are available.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

RADIUS accounting error

Symptom

A user is authenticated and authorized, but accounting for the user is not normal.

Analysis

The accounting server configuration on the NAS is not correct. Possible reasons include:

- The accounting port number configured on the NAS is incorrect.
- The accounting server IP address configured on the NAS is incorrect. For example, the NAS is configured to use a single server to provide authentication, authorization, and accounting services, but in fact the services are provided by different servers.

Solution

To resolve the problem:

1. Check the following items:
 - The accounting port number is correctly configured.
 - The accounting server IP address is correctly configured on the NAS.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

Troubleshooting HWTACACS

Similar to RADIUS troubleshooting. See "[Troubleshooting RADIUS](#)."

Troubleshooting LDAP

Symptom

User authentication fails.

Analysis

Possible reasons include:

- A communication failure exists between the NAS and the LDAP server.
- The LDAP server IP address or port number configured on the NAS is not correct.
- The username is not in the *userid@isp-name* format, or the ISP domain is not correctly configured on the NAS.
- The user is not configured on the LDAP server.
- The password entered by the user is incorrect.
- The administrator DN or password is not configured.
- Some user attributes (for example, the username attribute) configured on the NAS are not consistent with those configured on the server.
- No user search base DN is specified for the LDAP scheme.

Solution

To resolve the problem:

1. Check the following items:
 - The NAS and the LDAP server can ping each other.
 - The IP address and port number of the LDAP server configured on the NAS match those of the server.
 - The username is in the correct format and the ISP domain for the user authentication is correctly configured on the NAS.
 - The user is configured on the LDAP server.
 - The correct password is entered.
 - The administrator DN and the administrator password are correctly configured.
 - The user attributes (for example, the username attribute) configured on the NAS are consistent with those configured on the LDAP server.
 - The user search base DN for authentication is specified.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

802.1X overview

802.1X is a port-based network access control protocol initially proposed for securing WLANs. The protocol has also been widely used on Ethernet networks for access control.

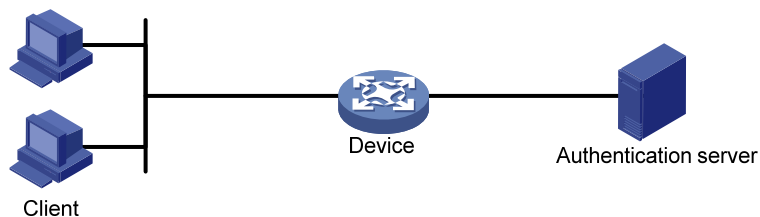
802.1X controls network access by authenticating the devices connected to 802.1X-enabled LAN ports.

802.1X architecture

802.1X operates in the client/server model. As shown in [Figure 28](#), 802.1X authentication includes the following entities:

- **Client (supplicant)**—A user terminal seeking access to the LAN. The terminal must have 802.1X software to authenticate to the access device.
- **Access device (authenticator)**—Authenticates the client to control access to the LAN. In a typical 802.1X environment, the access device uses an authentication server to perform authentication.
- **Authentication server**—Provides authentication services for the access device. The authentication server first authenticates 802.1X clients by using the data sent from the access device. Then, the server returns the authentication results to the access device to make access decisions. The authentication server is typically a RADIUS server. In a small LAN, you can use the access device as the authentication server.

Figure 28 802.1X architecture

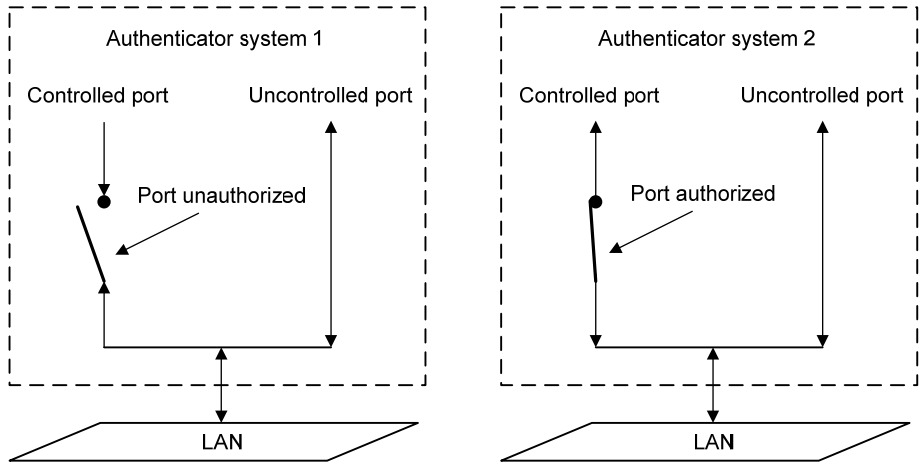


Controlled/uncontrolled port and port authorization status

802.1X defines two logical ports for the network access port: controlled port and uncontrolled port. Any packet arriving at the network access port is visible to both logical ports.

- **Uncontrolled port**—Is always open to receive and transmit authentication packets.
- **Controlled port**—Filters packets depending on the port state.
 - **Authorized state**—The controlled port is in authorized state when the client has passed authentication. The port allows traffic to pass through.
 - **Unauthorized state**—The port is in unauthorized state when the client has failed authentication. The port controls traffic by using one of the following methods:
 - Performs bidirectional traffic control to deny traffic to and from the client.
 - Performs unidirectional traffic control to deny traffic from the client. The HPE devices support only unidirectional traffic control.

Figure 29 Authorization state of a controlled port



802.1X-related protocols

802.1X uses the Extensible Authentication Protocol (EAP) to transport authentication information for the client, the access device, and the authentication server. EAP is an authentication framework that uses the client/server model. The framework supports a variety of authentication methods, including MD5-Challenge, EAP-Transport Layer Security (EAP-TLS), and Protected EAP (PEAP).

802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the access device over a wired or wireless LAN. Between the access device and the authentication server, 802.1X delivers authentication information by using one of the following methods:

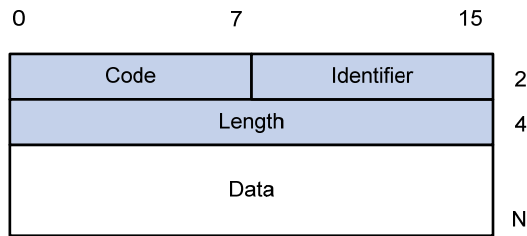
- Encapsulates EAP packets in RADIUS by using EAP over RADIUS (EAPOR), as described in "EAP relay."
- Extracts authentication information from the EAP packets and encapsulates the information in standard RADIUS packets, as described in "EAP termination."

Packet formats

EAP packet format

Figure 30 shows the EAP packet format.

Figure 30 EAP packet format



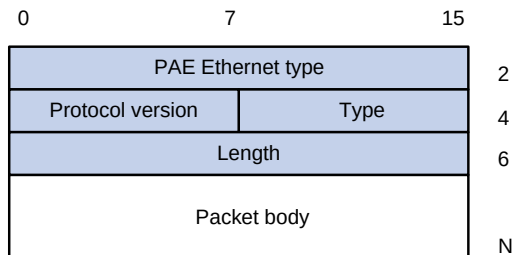
- **Code**—Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- **Identifier**—Used for matching Responses with Requests.
- **Length**—Length (in bytes) of the EAP packet. The EAP packet length is the sum of the Code, Identifier, Length, and Data fields.

- **Data**—Content of the EAP packet. This field appears only in a Request or Response EAP packet. The Data field contains the request type (or the response type) and the type data. Type 1 (Identify) and type 4 (MD5-challenge) are two examples for the type field.

EAPOL packet format

Figure 31 shows the EAPOL packet format.

Figure 31 EAPOL packet format



- **PAE Ethernet type**—Protocol type. It takes the value 0x888E for EAPOL.
- **Protocol version**—The EAPOL protocol version used by the EAPOL packet sender.
- **Type**—Type of the EAPOL packet. Table 4 lists the types of EAPOL packets supported by Hewlett Packard Enterprise implementation of 802.1X.

Table 4 Types of EAPOL packets

Value	Type	Description
0x00	EAP-Packet	The client and the access device uses EAP-Packets to transport authentication information.
0x01	EAPOL-Start	The client sends an EAPOL-Start message to initiate 802.1X authentication to the access device.
0x02	EAPOL-Logoff	The client sends an EAPOL-Logoff message to tell the access device that the client is logging off.

- **Length**—Data length in bytes, or length of the Packet body. If packet type is EAPOL-Start or EAPOL-Logoff, this field is set to 0, and no Packet body field follows.
- **Packet body**—Content of the packet. When the EAPOL packet type is EAP-Packet, the Packet body field contains an EAP packet.

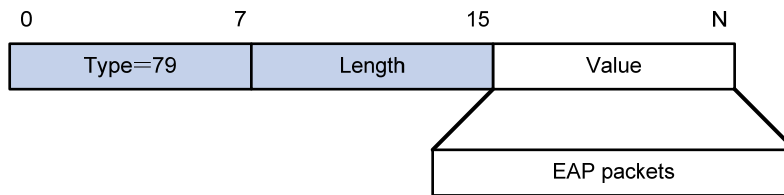
EAP over RADIUS

RADIUS adds two attributes, EAP-Message and Message-Authenticator, for supporting EAP authentication. For the RADIUS packet format, see "Configuring AAA."

EAP-Message

RADIUS encapsulates EAP packets in the EAP-Message attribute, as shown in Figure 32. The Type field takes 79, and the Value field can be up to 253 bytes. If an EAP packet is longer than 253 bytes, RADIUS encapsulates it in multiple EAP-Message attributes.

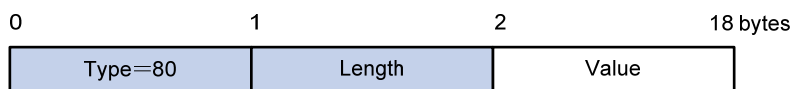
Figure 32 EAP-Message attribute format



Message-Authenticator

As shown in [Figure 33](#), RADIUS includes the Message-Authenticator attribute in all packets that have an EAP-Message attribute to check their integrity. The packet receiver drops the packet if the calculated packet integrity checksum is different from the Message-Authenticator attribute value. The Message-Authenticator prevents EAP authentication packets from being tampered with during EAP authentication.

Figure 33 Message-Authenticator attribute format



802.1X authentication initiation

Both the 802.1X client and the access device can initiate 802.1X authentication.

802.1X client as the initiator

The client sends an EAPOL-Start packet to the access device to initiate 802.1X authentication. The destination MAC address of the packet is the IEEE 802.1X specified multicast address 01-80-C2-00-00-03 or the broadcast MAC address. If any intermediate device between the client and the authentication server does not support the multicast address, you must use an 802.1X client that can send broadcast EAPOL-Start packets.

The broadcast trigger mode is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
 - HMIM-8GSW.
 - HMIM-24GSW.
 - HMIM-24GSWP.
 - SIC-4GSW.
 - SIC-4GSWP.
- Fixed Layer 2 Ethernet ports on the following routers:
 - MSR954(JH296A/JH297A/JH298A/JH299A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

Access device as the initiator

The access device initiates authentication, if a client cannot send EAPOL-Start packets. One example is the 802.1X client available with Windows XP.

The access device supports the following modes:

- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets to initiate 802.1X authentication at the identity request interval.
- **Unicast trigger mode**—Upon receiving a frame from an unknown MAC address, the access device sends an Identity EAP-Request packet out of the receiving port to the MAC address. The device retransmits the packet if no response has been received within the identity request timeout interval. This process continues until the maximum number of request attempts set by using the **dot1x retry** command is reached.

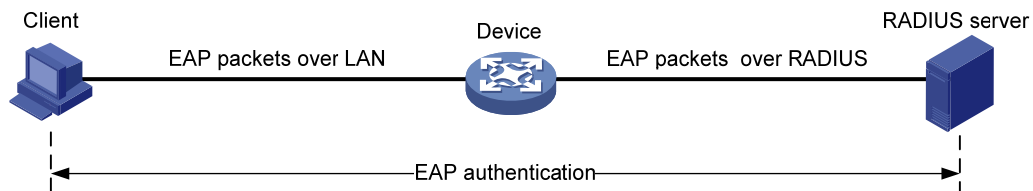
The username request timeout timer sets both the identity request interval for the multicast trigger and the identity request timeout interval for the unicast trigger.

802.1X authentication procedures

802.1X authentication has two methods: EAP relay and EAP termination. You choose either mode depending on support of the RADIUS server for EAP packets and EAP authentication methods.

- EAP relay mode.
EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAPOR packets to send authentication information to the RADIUS server, as shown in [Figure 34](#).

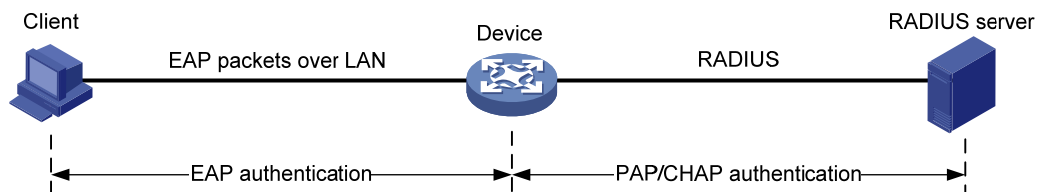
Figure 34 EAP relay



In EAP relay mode, the client must use the same authentication method as the RADIUS server. On the access device, you only need to use the **dot1x authentication-method eap** command to enable EAP relay.

- EAP termination mode.
As shown in [Figure 35](#), the access device performs the following operations in EAP termination mode:
 - Terminates the EAP packets received from the client.
 - Encapsulates the client authentication information in standard RADIUS packets.
 - Uses PAP or CHAP to authenticate to the RADIUS server.

Figure 35 EAP termination



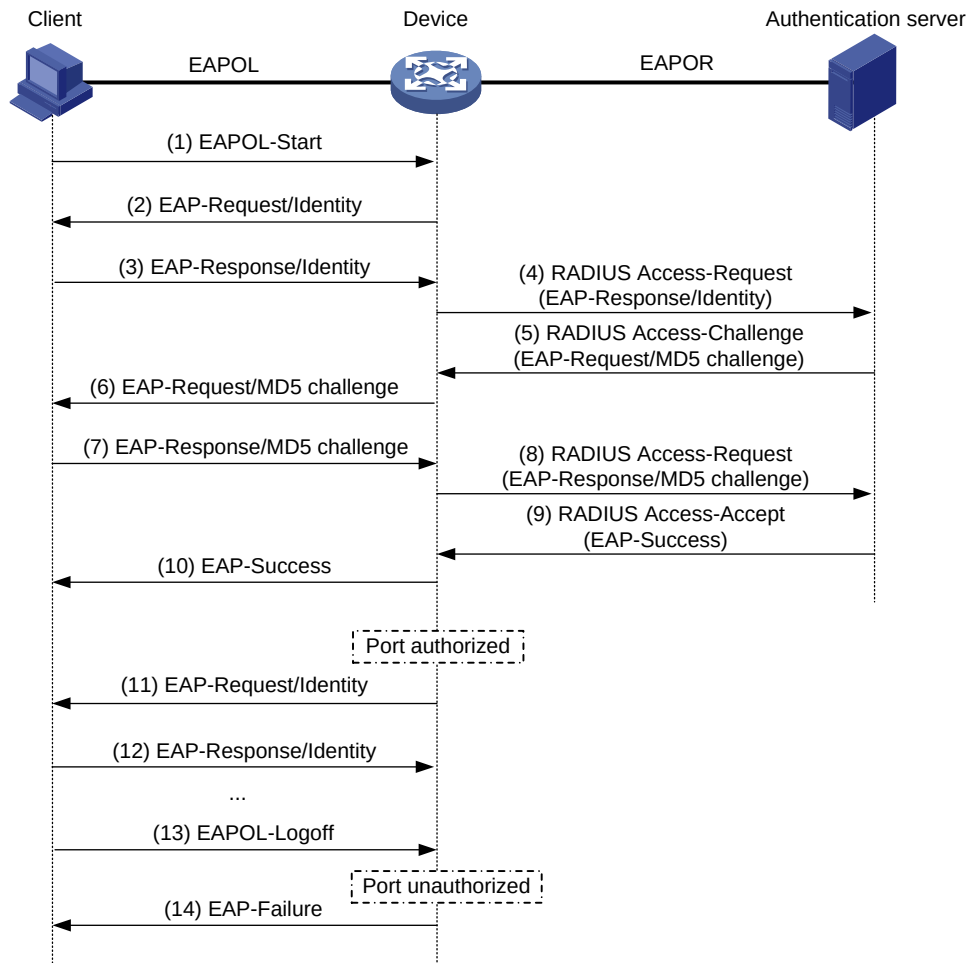
Comparing EAP relay and EAP termination

Packet exchange method	Benefits	Limitations
EAP relay	• Supports various EAP authentication methods. • The configuration and processing are simple on the access device.	The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client.
EAP termination	Works with any RADIUS server that supports PAP or CHAP authentication.	• Supports only the following EAP authentication methods: ◦ MD5-Challenge EAP authentication. ◦ The username and password EAP authentication initiated by an HPE iNode 802.1X client. • The processing is complex on the access device.

EAP relay

Figure 36 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

Figure 36 802.1X authentication procedure in EAP relay mode



The following steps describe the 802.1X authentication procedure:

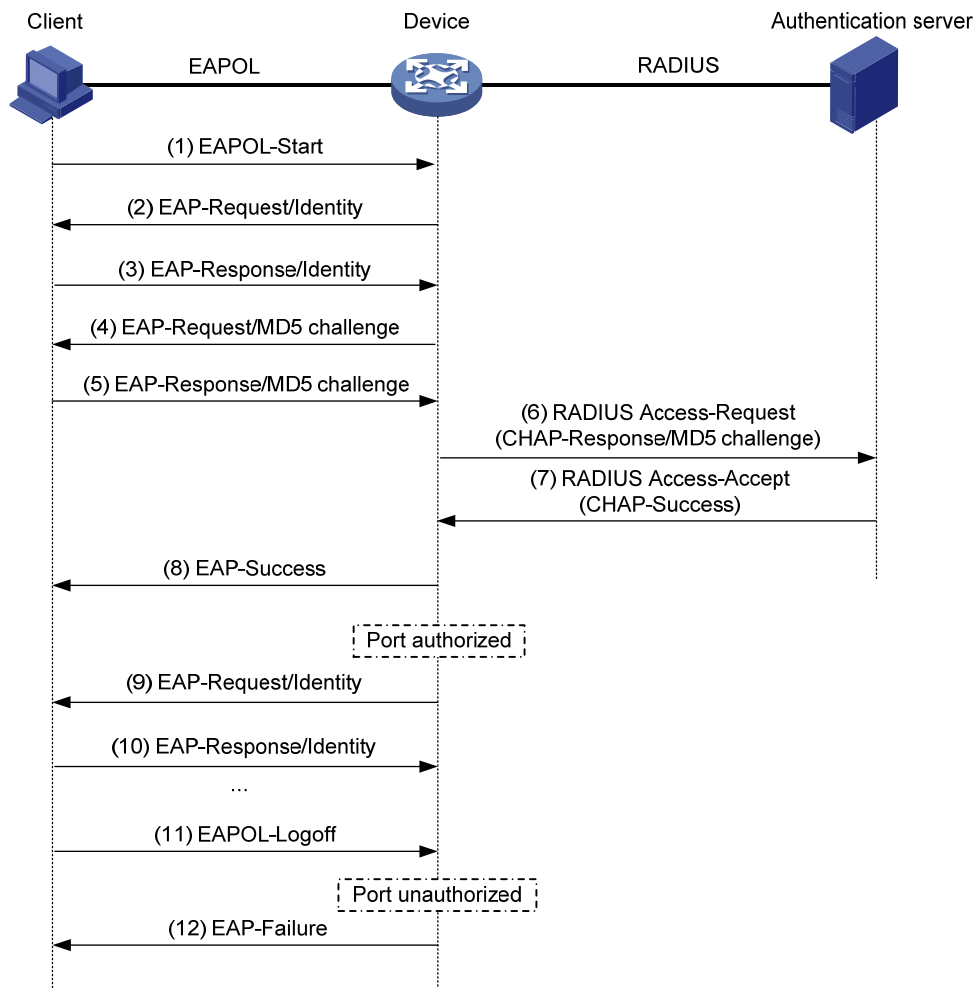
1. When a user launches the 802.1X client and enters a registered username and password, the 802.1X client sends an EAPOL-Start packet to the access device.
2. The access device responds with an Identity EAP-Request packet to ask for the client username.
3. In response to the Identity EAP-Request packet, the client sends the username in an Identity EAP-Response packet to the access device.
4. The access device relays the Identity EAP-Response packet in a RADIUS Access-Request packet to the authentication server.
5. The authentication server uses the identity information in the RADIUS Access-Request to search its user database. If a matching entry is found, the server uses a randomly generated challenge (EAP-Request/MD5 challenge) to encrypt the password in the entry. Then, the server sends the challenge in a RADIUS Access-Challenge packet to the access device.
6. The access device transmits the EAP-Request/MD5 Challenge packet to the client.
7. The client uses the received challenge to encrypt the password, and sends the encrypted password in an EAP-Response/MD5 Challenge packet to the access device.
8. The access device relays the EAP-Response/MD5 Challenge packet in a RADIUS Access-Request packet to the authentication server.
9. The authentication server compares the received encrypted password with the encrypted password it generated at step 5. If the two passwords are identical, the server considers the client valid and sends a RADIUS Access-Accept packet to the access device.

- 10.** Upon receiving the RADIUS Access-Accept packet, the access device performs the following operations:
 - a.** Sends an EAP-Success packet to the client.
 - b.** Sets the controlled port in authorized state.The client can access the network.
- 11.** After the client comes online, the access device periodically sends handshake requests to check whether the client is still online. By default, if two consecutive handshake attempts fail, the device logs off the client.
- 12.** Upon receiving a handshake request, the client returns a response. If the client fails to return a response after a number of consecutive handshake attempts (two by default), the access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users who have abnormally gone offline.
- 13.** The client can also send an EAPOL-Logoff packet to ask the access device for a logoff.
- 14.** In response to the EAPOL-Logoff packet, the access device changes the status of the controlled port from authorized to unauthorized. Then, the access device sends an EAP-Failure packet to the client.

EAP termination

Figure 37 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 37 802.1X authentication procedure in EAP termination mode



In EAP termination mode, the access device rather than the authentication server generates an MD5 challenge for password encryption. The access device then sends the MD5 challenge together with the username and encrypted password in a standard RADIUS packet to the RADIUS server.

Configuring 802.1X

This chapter describes how to configure 802.1X on an HPE device. You can also configure the port security feature to perform 802.1X. Port security combines and extends 802.1X and MAC authentication. It applies to a network, a WLAN, for example, that requires different authentication methods for different users on a port. For more information about the port security feature, see "[Configuring port security](#)."

Access control methods

Hewlett Packard Enterprise implements port-based access control as defined in the 802.1X protocol, and extends the protocol to support MAC-based access control.

- **Port-based access control**—Once an 802.1X user passes authentication on a port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.
- **MAC-based access control**—Each user is separately authenticated on a port. When a user logs off, no other online users are affected.

802.1X VLAN manipulation

Authorization VLAN

You can specify authorization VLANs for an 802.1X user to control access to authorized network resources. When the 802.1X user passes authentication, the authentication server assigns the authorization VLANs or VLAN group to the users.

Supported VLAN types and forms

Which VLAN types and forms are supported depends on the authorization type.

- Local VLAN authorization.
You can specify only one authorization VLAN by its ID in user view or user group view on the access device. For more information about local user configuration, see "[Configuring AAA](#)."
- Remote VLAN authorization.
You can specify a VLAN or a group of VLANs on the AAA server for 802.1X users. The access device supports VLANs of the following forms:
 - VLAN ID.
 - VLAN name.
The VLAN name represents the VLAN description on the access device.
 - Combination of VLAN IDs and VLAN names.
In the string, some VLANs are represented by their IDs, and some VLANs are represented by their names.
 - VLAN group name.
For more information about VLAN groups, see *Layer 2—LAN Switching Configuration Guide*.
 - VLAN ID with suffix.
The suffix can be **t** or **u**, which indicates whether the ports assigned to the VLAN are tagged members or not. For example, **2u** indicates that the ports assigned to VLAN 2 are untagged members.

NOTE:

The access device converts VLAN names and VLAN group name into VLAN IDs before VLAN assignment.

Unsupported VLAN types

Do not specify the following types of VLANs for VLAN authorization. The access device does not assign these VLANs to 802.1X users.

- VLANs that have not been created.
- Dynamically-learned VLANs.
- Reserved VLANs.
- Super VLANs.
- Private VLANs.

VLAN selection and assignment

If the server assigns a group of VLANs, the access device selects and assigns a VLAN according to the VLAN ID format. [Table 5](#) describes the VLAN selection and assignment rules for a group of authorization VLANs.

Table 5 VLAN selection and assignment for a group of authorization VLANs

Types of authorized VLANs	VLAN selection and assignment rules
• VLANs by IDs • VLANs by names • VLAN group name	The device selects a VLAN to be the authorization VLAN of a user, depending on whether the port has other online users: • If the port does not have other online users, the device selects the VLAN with the lowest ID from the group of VLANs. • If the port has other online users, the device selects the VLAN by using the following process: a. The device selects the VLAN that has the fewest number of online users. b. If two VLANs have the same number of online 802.1X users, the device selects the VLAN with the lower ID. The device follows the rules in Table 6 to handle VLAN assignment.
VLAN IDs with suffixes	1. The device selects the leftmost VLAN ID without a suffix, or the leftmost VLAN ID suffixed by u as an untagged VLAN, whichever is more leftmost. 2. The device assigns the untagged VLAN to the port as the PVID, and it assigns the remaining as tagged VLANs. If no untagged VLAN is assigned, the PVID of the port does not change. The port permits traffic from these tagged and untagged VLANs to pass through. For example, the authentication server sends the string 1u 2t 3 to the access device for a user. The device assigns VLAN 1 as an untagged VLAN and other VLANs as tagged VLANs. VLAN 1 becomes the PVID.

NOTE:

Assign VLAN IDs with suffixes only to hybrid or trunk ports that perform port-based access control.

[Table 6](#) describes how the access device handles VLANs (except for the VLANs specified with suffixes) on an 802.1X-enabled port.

Table 6 VLAN manipulation

Port access control method	VLAN manipulation
Port-based	The device assigns the first authenticated user's authorization VLAN to the port as the port VLAN (PVID). All subsequent 802.1X users can access the VLAN without authentication. When the first authenticated user logs off, the previous PVID is restored, and all other online users are logged off.
MAC-based	The device assigns the first authenticated user's authorization VLAN to the port as the PVID. If a different VLAN is authorized to a subsequent user, the user cannot pass the authentication. To ensure successful authentication of subsequent users, authorize the same VLAN to all 802.1X users on these ports.

A hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

For more information about VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Guest VLAN

The 802.1X guest VLAN on a port accommodates users who have not performed 802.1X authentication. Users in the guest VLAN can access a limited set of network resources, such as a software server, to download antivirus software and system patches. Once a user in the guest VLAN passes 802.1X authentication, it is removed from the guest VLAN and can access authorized network resources.

The 802.1X guest VLAN takes effect only on a port that performs port-based access control.

The following table illustrates how the access device handles VLANs on an 802.1X-enabled port that performs port-based access control:

Authentication status	VLAN manipulation
A user has not passed 802.1X authentication.	The device assigns the 802.1X guest VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the guest VLAN. If no 802.1X guest VLAN is configured, the access device does not perform any VLAN operation.
A user in the 802.1X guest VLAN fails 802.1X authentication.	If an 802.1X Auth-Fail VLAN (see "Auth-Fail VLAN") is available, the device assigns the Auth-Fail VLAN to the port as the PVID. All users on this port can access only resources in the Auth-Fail VLAN. If no Auth-Fail VLAN is configured, the PVID on the port is still the 802.1X guest VLAN. All users on the port are in the guest VLAN.
A user in the 802.1X guest VLAN passes 802.1X authentication.	- The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X guest VLAN. After the user logs off, the initial PVID of the port is restored. - If the authentication server does not authorize a VLAN, the initial PVID applies. The user and all subsequent 802.1X users are assigned to the initial port VLAN. After the user logs off, the port VLAN remains unchanged. NOTE: The initial PVID of an 802.1X-enabled port refers to the PVID used by the port before the port is assigned to any 802.1X VLANs.

The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member.

For more information about VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Auth-Fail VLAN

The 802.1X Auth-Fail VLAN on a port accommodates users who have failed 802.1X authentication because of the failure to comply with the organization security strategy. For example, the VLAN accommodates users who have entered a wrong password. Users in the Auth-Fail VLAN can access a limited set of network resources, such as a software server, to download antivirus software and system patches.

The Auth-Fail VLAN does not accommodate 802.1X users who have failed authentication for authentication timeouts or network connection problems.

The 802.1X Auth-Fail VLAN takes effect only on a port that performs port-based access control.

The following table illustrates how the access device handles VLANs on an 802.1X-enabled port that performs port-based access control:

Authentication status	VLAN manipulation
A user fails 802.1X authentication.	The device assigns the Auth-Fail VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the Auth-Fail VLAN.
A user in the 802.1X Auth-Fail VLAN fails 802.1X authentication because of any other reason except for unreachable servers.	The Auth-Fail VLAN is still the PVID on the port, and all 802.1X users on this port are in this VLAN.
A user passes 802.1X authentication.	- The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the Auth-Fail VLAN. After the user logs off, the guest VLAN is assigned to the port as the PVID. If no guest VLAN is configured, the initial PVID of the port is restored. - If the authentication server does not authorize a VLAN, the initial PVID of the port applies. The user and all subsequent 802.1X users are assigned to the initial PVID. After the user logs off, the PVID remains unchanged.

The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member.

For more information about VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Critical VLAN

The 802.1X critical VLAN on a port accommodates 802.1X users who have failed authentication because none of the RADIUS servers in their ISP domain is reachable. Users in the critical VLAN can access a limited set of network resources depending on the configuration.

The critical VLAN feature takes effect when 802.1X authentication is performed only through RADIUS servers. If an 802.1X user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN. For more information about the authentication methods, see ["Configuring AAA."](#)

The 802.1X critical VLAN takes effect only on a port that performs port-based access control.

The following table illustrates how the access device handles VLANs on an 802.1X-enabled port that performs port-based access control:

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	The device assigns the critical VLAN to the port as the PVID. The 802.1X user and all subsequent 802.1X users on this port can access only resources in the 802.1X critical VLAN.

Authentication status	VLAN manipulation
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The critical VLAN is still the PVID of the port, and all 802.1X users on this port are in this VLAN.
A user in the 802.1X critical VLAN fails authentication for any other reasons except for unreachable servers.	If an 802.1X Auth-Fail VLAN has been configured, the PVID of the port changes to the Auth-Fail VLAN ID, and all 802.1X users on this port are moved to the Auth-Fail VLAN. If no 802.1X Auth-Fail VLAN is configured, the initial PVID of the port is restored.
A user in the 802.1X critical VLAN passes 802.1X authentication.	- The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X critical VLAN. After the user logs off, the guest VLAN ID changes to the PVID. If no 802.1X guest VLAN is configured, the initial PVID of the port is restored. - If the authentication server (either the local access device or a RADIUS server) does not authorize a VLAN, the initial PVID of the port applies. The user and all subsequent 802.1X users are assigned to this port VLAN. After the user logs off, the PVID remains unchanged.
A user in the 802.1X guest VLAN fails authentication because all the RADIUS servers are unreachable.	The device assigns the 802.1X critical VLAN to the port as the PVID, and all 802.1X users on this port are in this VLAN.
A user in the 802.1X Auth-Fail VLAN fails authentication because all the RADIUS servers are unreachable.	The PVID of the port remains unchanged. All 802.1X users on this port can access only resources in the 802.1X Auth-Fail VLAN.
A user who has passed authentication fails reauthentication because all the RADIUS servers are unreachable, and the user is logged out of the device.	The device assigns the 802.1X critical VLAN to the port as the PVID.

The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member.

When a reachable RADIUS server is detected, the device removes the port from the critical VLAN. The port sends a multicast Identity EAP/Request to all 802.1X users on the port to trigger authentication.

For more information about VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Using 802.1X authentication with other features

ACL assignment

You can specify an ACL for an 802.1X user to control the user's access to network resources. After the user passes 802.1X authentication, the authentication server assigns the ACL to the access port to filter traffic from this user. The authentication server can be the local access device or a RADIUS server. In either case, you must configure the ACL on the access device.

To change the access control criteria for the user, you can use one of the following methods:

- Modify ACL rules on the access device.
- Specify another authorization ACL on the authentication server.

For more information about ACLs, see *ACL and QoS Configuration Guide*.

EAD assistant

Endpoint Admission Defense (EAD) is an Hewlett Packard Enterprise integrated endpoint access control solution to improve the threat defensive capability of a network. The solution enables the security client, security policy server, access device, and third-party server to operate together. If a terminal device seeks to access an EAD network, it must have an EAD client, which performs 802.1X authentication.

The EAD assistant feature enables the access device to redirect a user who is seeking to access the network to download and install an EAD client. This feature eliminates the administrative task to deploy EAD clients.

EAD assistant is implemented by the following functionality:

- Free IP.
A free IP is a freely accessible network segment, which has a limited set of network resources such as software and DHCP servers. To ensure security strategy compliance, an unauthenticated user can access only this segment to perform operations. For example, the user can download EAD client from a software server or obtain a dynamic IP address from a DHCP server.
- Redirect URL.
If an unauthenticated 802.1X user is using a Web browser to access the network, the EAD assistant feature redirects the user to a specific URL. For example, you can use this feature to redirect the user to the EAD client software download page.

The EAD assistant feature creates an ACL-based EAD rule automatically to open access to the redirect URL for each redirected user.

EAD rules are implemented by using ACL resources. When the EAD rule timer expires or the user passes authentication, the rule is removed. If users fail to download EAD client or fail to pass authentication before the timer expires, they must reconnect to the network to access the free IP.

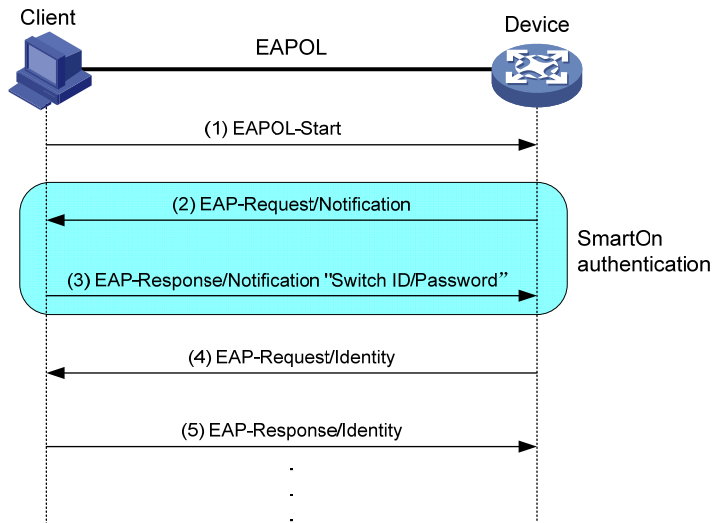
SmartOn

The SmartOn feature was developed to support the NEC 802.1X client.

As shown in [Figure 38](#), the access device performs SmartOn authentication before 802.1X authentication. The following shows the authentication process:

1. When a SmartOn-enabled port receives an EAPOL-Start packet from an 802.1X client, it sends a unicast EAP-Request/Notification packet to the client for SmartOn authentication.
2. Upon receiving an EAP-Response/Notification from the client, the device compares the switch ID and password in the packet with the switch ID and password configured on the device.
 - If they are the same, 802.1X authentication can continue.
 - If they do not match, SmartOn authentication fails. The access device stops 802.1X authentication for the client.

Figure 38 802.1X authentication process with the SmartOn feature



If the user attempts to use another 802.1X client for authentication, it will fail SmartOn authentication. The access device stops 802.1X authentication for the user.

NOTE:

After you install the SmartOn client software, add two values **QX_ID** and **QX_PASSWORD** to the Windows registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Soliton Systems K.K.\SmartOn Client\Clients\1XGate]. Specify the switch ID and password for the QX_ID and QX_PASSWORD, respectively. The switch ID and password must be the same as the switch ID and password configured on the device.

Compatibility information

Feature and hardware compatibility

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
 - MSR954(JH296A/JH297A/JH298A/JH299A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Configuration prerequisites

Before you configure 802.1X, complete the following tasks:

- Configure an ISP domain and AAA scheme (local or RADIUS authentication) for 802.1X users.
- If RADIUS authentication is used, create user accounts on the RADIUS server.
- If local authentication is used, create local user accounts on the access device and set the service type to **lan-access**.

802.1X configuration task list

Tasks at a glance
(Required.) Enabling 802.1X
(Required.) Enabling EAP relay or EAP termination
(Optional.) Setting the port authorization state
(Optional.) Specifying an access control method
(Optional.) Setting the maximum number of concurrent 802.1X users on a port
(Optional.) Setting the maximum number of authentication request attempts
(Optional.) Setting the 802.1X authentication timeout timers
(Optional.) Configuring the online user handshake feature
(Optional.) Configuring the authentication trigger feature
(Optional.) Specifying a mandatory authentication domain on a port
(Optional.) Setting the quiet timer
(Optional.) Enabling the periodic online user reauthentication feature
(Optional.) Configuring an 802.1X guest VLAN
(Optional.) Configuring an 802.1X Auth-Fail VLAN
(Optional.) Configuring an 802.1X critical VLAN
(Optional.) Specifying supported domain name delimiters
(Optional.) Configuring the EAD assistant feature
(Optional.) Configuring 802.1X SmartOn

Enabling 802.1X

When you enable 802.1X, follow these guidelines:

- Do not enable 802.1X on a port that is in a link aggregation or service loopback group.
- You can enable both 802.1X authentication and portal authentication (except for re-DHCP authentication) on a Layer 3 interface. A user who passes either authentication can come online. If you enable re-DHCP portal authentication on an 802.1X-enabled Layer 3 interface, portal authentication always fails. For more information about portal configuration, see "[Configuring portal authentication](#)."

To enable 802.1X:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable 802.1X globally.	dot1x	By default, 802.1X is disabled globally.
3. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable 802.1X on a port.	dot1x	By default, 802.1X is disabled on a port.

Enabling EAP relay or EAP termination

When configuring EAP relay or EAP termination, consider the following factors:

- Support of the RADIUS server for EAP packets.
- Authentication methods supported by the 802.1X client and the RADIUS server.

You can use both EAP termination and EAP relay in any of the following situations:

- The client is using only MD5-Challenge EAP authentication.
- The client is using only the username and password EAP authentication initiated by an HPE iNode 802.1X client.

To use EAP-TL, PEAP, or any other EAP authentication methods, you must use EAP relay. When you make your decision, see "[Comparing EAP relay and EAP termination](#)" for help.

For more information about EAP relay and EAP termination, see "[802.1X authentication procedures](#)."

To configure EAP relay or EAP termination:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure EAP relay or EAP termination.	dot1x authentication-method { chap eap pap }	By default, the access device performs EAP termination and uses CHAP to communicate with the RADIUS server. Specify the eap keyword to enable EAP relay. Specify the chap or pap keyword to enable CHAP-enabled or PAP-enabled EAP termination.

NOTE:

If EAP relay mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. The access device sends the authentication data from the client to the server without any modification.

Setting the port authorization state

The port authorization state determines whether the client is granted access to the network. You can control the authorization state of a port by using the **dot1x port-control** command and the following keywords:

- **authorized-force**—Places the port in the authorized state, enabling users on the port to access the network without authentication.

- **unauthorized-force**—Places the port in the unauthorized state, denying any access requests from users on the port.
- **auto**—Places the port initially in unauthorized state to allow only EAPOL packets to pass. After a user passes authentication, sets the port in the authorized state to allow access to the network. You can use this option in most scenarios.

To set the authorization state of a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the port authorization state.	dot1x port-control { authorized-force auto unauthorized-force }	By default, the auto state applies.

Specifying an access control method

You can specify port-based or MAC-based access control method for 802.1X authentication. The MAC-based access control method is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
 - HMIM-8GSW.
 - HMIM-24GSW.
 - HMIM-24GSWP.
 - SIC-4GSW.
 - SIC-4GSWP.
- Fixed Layer 2 Ethernet ports on the following routers:
 - MSR954(JH296A/JH297A/JH298A/JH299A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

To specify an access control method:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify an access control method.	dot1x port-method { macbased portbased }	By default, MAC-based access control applies. To use both 802.1X and portal authentication on a port, you must specify MAC-based access control. For information about portal authentication, see "Configuring portal authentication."

Setting the maximum number of concurrent 802.1X users on a port

Perform this task to prevent the system resources from being overused.

To set the maximum number of concurrent 802.1X users on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the maximum number of concurrent 802.1X users on a port.	dot1x max-user <i>user-number</i>	The default setting is 4096.

Setting the maximum number of authentication request attempts

The access device retransmits an authentication request if it does not receive any responses to the request from the client within a period of time. To set the time, use the **dot1x timer tx-period** *tx-period-value* command or the **dot1x timer supp-timeout** *supp-timeout-value* command. The access device stops retransmitting the request if it has made the maximum number of request transmission attempts but still receives no response.

To set the maximum number of authentication request attempts:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the maximum number of attempts for sending an authentication request.	dot1x retry <i>max-retry-value</i>	The default setting is 2.

Setting the 802.1X authentication timeout timers

The network device uses the following 802.1X authentication timeout timers:

- **Client timeout timer**—Starts when the access device sends an EAP-Request/MD5 Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Server timeout timer**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

- In a low-speed network, increase the client timeout timer.
- In a network with authentication servers of different performance, adjust the server timeout timer.

To set the 802.1X authentication timeout timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the client timeout timer.	dot1x timer supp-timeout <i>supp-timeout-value</i>	The default is 30 seconds.
3. Set the server timeout timer.	dot1x timer server-timeout <i>server-timeout-value</i>	The default is 100 seconds.

Configuring the online user handshake feature

The online user handshake feature checks the connectivity status of online 802.1X users. The access device sends handshake messages to online users at the interval specified by the **dot1x timer handshake-period** command. If the device does not receive any responses from an online user after it has made the maximum handshake attempts, the device sets the user to offline state. To set the maximum handshake attempts, use the **dot1x retry** command.

If iNode clients are deployed, you can also enable the online user handshake security feature to check authentication information in the handshake packets from clients. This feature can prevent 802.1X users who use illegal client software from bypassing iNode security check, such as dual network interface cards (NICs) detection. If a user fails the handshake security checking, the device sets the user to the offline state.

Configuration guidelines

When you configure the online user handshake feature, follow these restrictions and guidelines:

- The SmartOn feature and the online user handshake feature are mutually exclusive. Before you enable the online user handshake feature, make sure the SmartOn feature is disabled.
- To use the online user handshake security feature, make sure the online user handshake feature is enabled.
- The online user handshake security feature takes effect only on the network where the iNode client and IMC server are used.
- If the network has 802.1X clients that cannot exchange handshake packets with the access device, disable the online user handshake feature. This operation prevents the 802.1X connections from being incorrectly torn down.

Configuration procedure

To configure the online user handshake feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Set the handshake timer.	dot1x timer handshake-period <i>handshake-period-value</i>	The default is 15 seconds.
3. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable the online user handshake feature.	dot1x handshake	By default, the feature is enabled.
5. (Optional.) Enable the online user handshake security feature.	dot1x handshake secure	By default, the feature is disabled.

Configuring the authentication trigger feature

The authentication trigger feature enables the access device to initiate 802.1X authentication when 802.1X clients cannot initiate authentication.

This feature provides the multicast trigger and unicast trigger (see 802.1X authentication initiation in "[802.1X overview](#)").

Configuration guidelines

When you configure the authentication trigger feature, follow these guidelines:

- Enable the multicast trigger on a port when the clients attached to the port cannot send EAPOL-Start packets to initiate 802.1X authentication.
- Enable the unicast trigger on a port if only a few 802.1X clients are attached to the port and these clients cannot initiate authentication.
- To avoid duplicate authentication packets, do not enable both triggers on a port.

Configuration procedure

To configure the authentication trigger feature on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Set the username request timeout timer.	dot1x timer tx-period <i>tx-period-value</i>	The default is 30 seconds.
3. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable an authentication trigger.	dot1x { multicast-trigger unicast-trigger }	By default, the multicast trigger is enabled, and the unicast trigger is disabled.

Specifying a mandatory authentication domain on a port

You can place all 802.1X users in a mandatory authentication domain for authentication, authorization, and accounting on a port. No user can use an account in any other domain to access the network through the port. The implementation of a mandatory authentication domain enhances the flexibility of 802.1X access control deployment.

To specify a mandatory authentication domain for a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify a mandatory 802.1X authentication domain on the port.	dot1x mandatory-domain <i>domain-name</i>	By default, no mandatory 802.1X authentication domain is specified.

Setting the quiet timer

The quiet timer enables the access device to wait a period of time before it can process any authentication request from a client that has failed an 802.1X authentication.

You can edit the quiet timer, depending on the network conditions.

- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.

To set the quiet timer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the quiet timer.	dot1x quiet-period	By default, the timer is disabled.
3. (Optional.) Set the quiet timer.	dot1x timer quiet-period <i>quiet-period-value</i>	The default is 60 seconds.

Enabling the periodic online user reauthentication feature

Periodic online user reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the server. The attributes include the ACL and VLAN. The reauthentication interval is user configurable.

The server-assigned session timeout timer (Session-Timeout attribute) and termination action (Termination-Action attribute) can affect the periodic online user reauthentication feature. To display the server-assigned Session-Timeout and Termination-Action attributes, use the **display dot1x connection** command (see *Security Command Reference*).

- If the termination action is **Default** (logoff), periodic online user reauthentication on the device takes effect only when the periodic reauthentication timer is shorter than the session timeout timer.
- If the termination action is **Radius-request**, the periodic online user reauthentication configuration on the device does not take effect. The device reauthenticates the online 802.1X users after the session timeout timer expires.

Support for the assignment of Session-Timeout and Termination-Action attributes depends on the server model.

The VLANs assigned to an online user before and after reauthentication can be the same or different.

To enable the periodic online user reauthentication feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Set the periodic reauthentication timer.	dot1x timer reauth-period <i>reauth-period-value</i>	The default is 3600 seconds.
3. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable periodic online user reauthentication.	dot1x re-authenticate	By default, the feature is disabled.

Step	Command	Remarks
5. (Optional.) Enable the keep-online feature for 802.1X users.	dot1x re-authenticate server-unreachable keep-online	By default, this feature is disabled. The device logs off online 802.1X users if no authentication server is reachable for 802.1X reauthentication.

Configuring an 802.1X guest VLAN

Configuration guidelines

When you configure an 802.1X guest VLAN, follow these guidelines:

- You cannot specify a VLAN as both a super VLAN and an 802.1X guest VLAN. For information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- You can configure only one 802.1X guest VLAN on a port. The 802.1X guest VLANs on different ports can be different.
- Assign different IDs to the port VLAN and the 802.1X guest VLAN on a port. The assignment ensures that the port can correctly process incoming VLAN-tagged traffic.
- Make sure the VLAN to be specified as the 802.1X guest VLAN already exists.

Configuration procedure

To configure an 802.1X guest VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the 802.1X guest VLAN on the port.	dot1x guest-vlan <i>guest-vlan-id</i>	By default, no 802.1X guest VLAN is configured on any port.

Configuring an 802.1X Auth-Fail VLAN

Configuration guidelines

When you configure an 802.1X Auth-Fail VLAN, follow these restrictions and guidelines:

- You cannot specify a VLAN as both a super VLAN and an 802.1X Auth-Fail VLAN. For information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- Assign different IDs to the port VLAN and the 802.1X Auth-Fail VLAN on a port. The assignment ensures that the port can correctly process VLAN-tagged incoming traffic.
- You can configure only one 802.1X Auth-Fail VLAN on a port. The 802.1X Auth-Fail VLANs on different ports can be different.
- Make sure the VLAN to be specified as the 802.1X Auth-Fail VLAN already exists.

Configuration procedure

To configure an 802.1X Auth-Fail VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the 802.1X Auth-Fail VLAN on the port.	dot1x auth-fail vlan <i>authfail-vlan-id</i>	By default, no 802.1X Auth-Fail VLAN is configured.

Configuring an 802.1X critical VLAN

Configuration guidelines

When you configure an 802.1X critical VLAN, follow these restrictions and guidelines:

- Assign different IDs to the port VLAN and the 802.1X critical VLAN on a port. The assignment ensures that the port can correctly process VLAN-tagged incoming traffic.
- You can configure only one 802.1X critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.
- You cannot specify a VLAN as both a super VLAN and an 802.1X critical VLAN. For information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- Make sure the VLAN to be specified as the 802.1X critical VLAN already exists.

Configuration procedure

To configure an 802.1X critical VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the 802.1X critical VLAN on the port.	dot1x critical vlan <i>vlan-id</i>	By default, no 802.1X critical VLAN is configured.

Specifying supported domain name delimiters

By default, the access device supports the at sign (@) as the delimiter. You can also configure the access device to accommodate 802.1X users who use other domain name delimiters. The configurable delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of *username@domain-name*, *domain-name\username*, *username.domain-name*, or *username/domain-name*.

If an 802.1X username string contains multiple configured delimiters, the rightmost delimiter is the domain name delimiter. For example, if you configure the backslash (\), dot (.), and forward slash (/) as delimiters, the domain name delimiter for the username string 121.123/22\@abc is the backslash (\). The username is @abc and the domain name is 121.123/22.

If a username string contains none of the delimiters, the access device authenticates the user in the mandatory or default ISP domain.

To specify a set of domain name delimiters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a set of domain name delimiters for 802.1X users.	dot1x domain-delimiter <i>string</i>	By default, only the at sign (@) delimiter is supported.

NOTE:

If you configure the access device to send usernames with domain names to the RADIUS server, make sure the domain delimiter can be recognized by the RADIUS server. For username format configuration, see the **user-name-format** command in *Security Command Reference*.

Configuring the EAD assistant feature

This feature is available only for the following routers:

- MSR954(JH296A/JH297A/JH298A/JH299A).
- MSR1002-4/1003-8S.
- MSR2004-24/2004-48.

When you configure the EAD assistant feature, follow these restrictions and guidelines:

- You must disable MAC authentication and port security globally before you enable the EAD assistant feature.
- To make the EAD assistant feature take effect on an 802.1X-enabled port, you must set the port authorization mode to **auto**.
- When global MAC authentication or port security is enabled, the free IP does not take effect.
- If you use free IP, guest VLAN, and Auth-Fail VLAN features together, make sure the free IP segments are in both guest VLAN and Auth-Fail VLAN.
- To allow a user to obtain a dynamic IP address before it passes 802.1X authentication, make sure the DHCP server is on the free IP segment.
- The server that provides the redirect URL must be on the free IP accessible to unauthenticated users.
- To avoid using up ACL resources when a large number of EAD users exist, you can shorten the EAD rule timer.

To configure the EAD assistant feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable EAD assistant.	dot1x ead-assistant enable	By default, this feature is disabled.
3. Configure a free IP.	dot1x ead-assistant free-ip <i>ip-address { mask-length mask-address }</i>	By default, no free IP is configured.

Step	Command	Remarks
4. (Optional.) Configure the redirect URL.	dot1x ead-assistant url <i>url-string</i>	By default, no redirect URL is configured. Configure the redirect URL if users will use Web browsers to access the network.
5. (Optional.) Set the EAD rule timer.	dot1x timer ead-timeout <i>ead-timeout-value</i>	The default setting is 30 minutes.

Configuring 802.1X SmartOn

The SmartOn feature is mutually exclusive with the 802.1X online user handshake feature.

When the device sends a unicast EAP-Request/Notification packet to the client, it starts the SmartOn client timeout timer (set by using the **dot1x smarton timer supp-timeout** command).

- If the device does not receive any EAP-Response/Notification packets from the client within the timeout timer, it retransmits the EAP-Request/Notification packet to the client. After the device has made the maximum retransmission attempts but received no response, it stops the 802.1X authentication process for the client.
- If the device receives an EAP-Response/Notification packet within the timer or before the maximum retransmission attempts have been made, it starts the SmartOn authentication. If the SmartOn switch ID and the MD5 digest of the SmartOn password in the packet match those on the device, 802.1X authentication continues for the client. Otherwise, the device denies the client's 802.1X authentication request.

To configure 802.1X SmartOn:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the SmartOn feature on the port.	dot1x smarton	By default, this feature is disabled.
4. Return to system view.	quit	N/A
5. Configure the SmartOn switch ID.	dot1x smarton switchid <i>switch-string</i>	By default, no SmartOn switch ID is configured.
6. Configure the SmartOn password.	dot1x smarton password { cipher <i>cipher-string</i> simple <i>plain-string</i> }	By default, no SmartOn password is configured.
7. (Optional.) Set the SmartOn client timeout timer.	dot1x smarton timer supp-timeout <i>supp-timeout-value</i>	The default timer is 30 seconds.
8. (Optional.) Set the maximum attempts for retransmitting an EAP-Request/Notification packet to a client.	dot1x smarton retry <i>retries</i>	By default, the device allows a maximum of 3 attempts for retransmitting an EAP-Request/Notification packet to a client.

Displaying and maintaining 802.1X

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display 802.1X session information, statistics, or configuration information of specified or all ports.	display dot1x [sessions statistics] [interface <i>interface-type interface-number</i>]
Display online 802.1X user information (centralized devices in standalone mode).	display dot1x connection [interface <i>interface-type interface-number</i> user-mac <i>mac-addr</i> user-name <i>name-string</i>]
Display online 802.1X user information (distributed devices in standalone mode/centralized devices in IRF mode).	display dot1x connection [interface <i>interface-type interface-number</i> slot <i>slot-number</i> user-mac <i>mac-addr</i> user-name <i>name-string</i>]
Display online 802.1X user information (distributed devices in IRF mode).	display dot1x connection [chassis <i>chassis-number</i> slot <i>slot-number</i> interface <i>interface-type interface-number</i> user-mac <i>mac-addr</i> user-name <i>name-string</i>]
Clear 802.1X statistics.	reset dot1x statistics [interface <i>interface-type interface-number</i>]
Remove users from the 802.1X guest VLAN on a port.	reset dot1x guest-vlan interface <i>interface-type interface-number</i> [mac-address <i>mac-address</i>]

802.1X authentication configuration examples

Basic 802.1X authentication configuration example

Network requirements

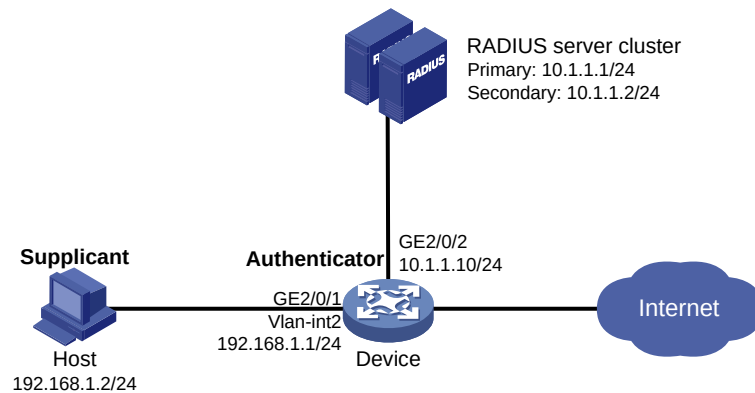
As shown in [Figure 39](#), the access device performs 802.1X authentication for users who connect to port GigabitEthernet 2/0/1. Implement MAC-based access control on the port, so the logoff of one user does not affect other online 802.1X users.

Use RADIUS servers to perform authentication, authorization, and accounting for the 802.1X users. If RADIUS authentication fails, perform local authentication on the access device.

Configure the host at 10.1.1.1/24 as the primary authentication and accounting servers, and the host at 10.1.1.2/24 as the secondary authentication and accounting servers. Assign all users to the ISP domain **bbb**.

Set the shared key to **name** for packets between the access device and the authentication server. Set the shared key to **money** for packets between the access device and the accounting server.

Figure 39 Network diagram



Configuration procedure

1. Configure the 802.1X client. If HPE iNode is used, do not select the **Carry version info** option in the client configuration. (Details not shown.)
2. Configure the RADIUS servers and add user accounts for the 802.1X users. (Details not shown.)

For information about the RADIUS commands used on the access device in this example, see *Security Command Reference*.

3. Assign an IP address for each interface on the access device. (Details not shown.)
4. Configure user accounts for the 802.1X users on the access device:

Add a local network access user with the username **localuser**, and password **localpass** in plaintext. (Make sure the username and password are the same as those configured on the RADIUS servers.)

```

<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
# Set the service type to lan-access.
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] quit
  
```

5. Configure a RADIUS scheme:

Create a RADIUS scheme named **radius1** and enter its view.

```
[Device] radius scheme radius1
```

Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[Device-radius-radius1] primary authentication 10.1.1.1
```

```
[Device-radius-radius1] primary accounting 10.1.1.1
```

Configure the IP addresses of the secondary authentication and accounting RADIUS servers.

```
[Device-radius-radius1] secondary authentication 10.1.1.2
```

```
[Device-radius-radius1] secondary accounting 10.1.1.2
```

Specify the shared key between the access device and the authentication server.

```
[Device-radius-radius1] key authentication simple name
```

Specify the shared key between the access device and the accounting server.

```
[Device-radius-radius1] key accounting simple money
```

Exclude the ISP domain names from the usernames sent to the RADIUS servers.

```
[Device-radius-radius1] user-name-format without-domain
```

```
[Device-radius-radius1] quit
```

NOTE:

The access device must use the same username format as the RADIUS server. If the RADIUS server includes the ISP domain name in the username, so must the access device.

6. Configure the ISP domain:

Create an ISP domain named **bbb** and enter its view.

```
[Device] domain bbb
```

Apply the RADIUS scheme **radius1** to the ISP domain, and specify local authentication as the secondary authentication method.

```
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
```

```
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
```

```
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
```

```
[Device-isp-bbb] quit
```

7. Configure 802.1X:

Enable 802.1X on GigabitEthernet 2/0/1.

```
[Device] interface gigabitethernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] dot1x
```

Enable MAC-based access control on the port. By default, the port uses MAC-based access control.

```
[Device-GigabitEthernet2/0/1] dot1x port-method macbased
```

Specify the ISP domain **bbb** as the mandatory domain.

```
[Device-GigabitEthernet2/0/1] dot1x mandatory-domain bbb
```

```
[Device-GigabitEthernet2/0/1] quit
```

Enable 802.1X globally.

```
[Device] dot1x
```

Verifying the configuration

Verify the 802.1X configuration on GigabitEthernet 2/0/1.

```
[Device] display dot1x interface gigabitethernet 2/0/1
```

Display the user connection information after an 802.1X user passes authentication.

```
[Device] display dot1x connection
```

802.1X guest VLAN and authorization VLAN configuration example

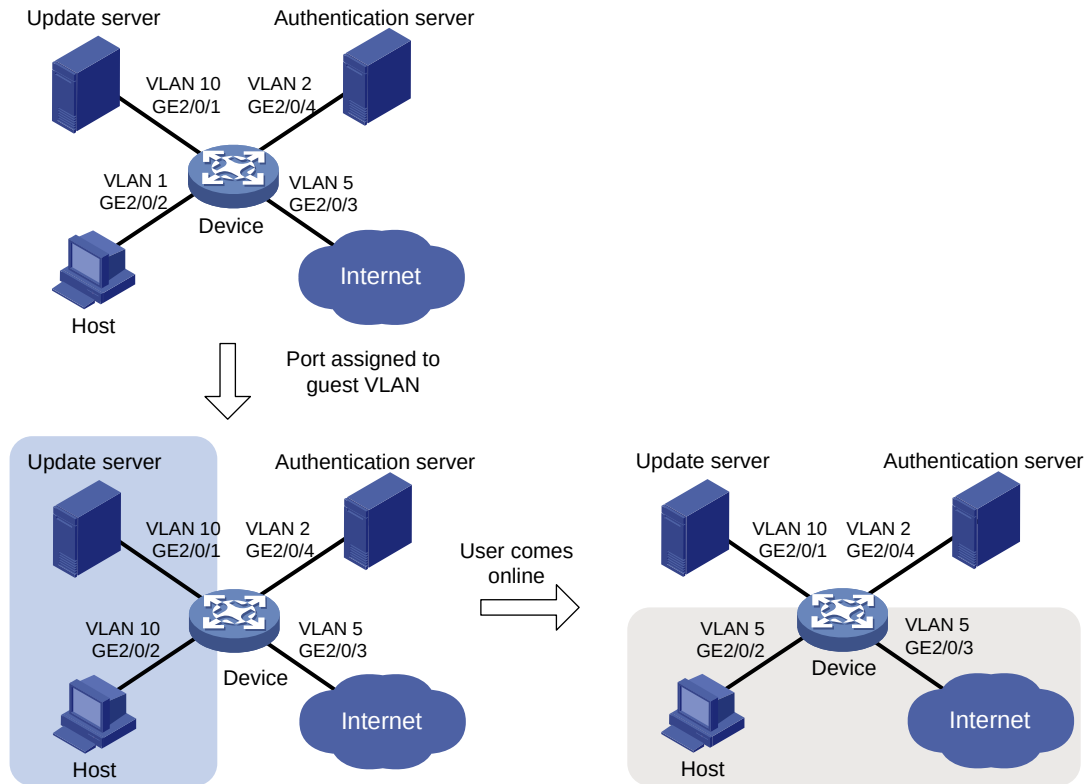
Network requirements

As shown in [Figure 40](#), use RADIUS servers to perform authentication, authorization, and accounting for 802.1X users who connect to GigabitEthernet 2/0/2. Implement port-based access control on the port.

Configure VLAN 10 as the 802.1X guest VLAN on GigabitEthernet 2/0/2. The host and the update server are both in VLAN 10, and the host can access the update server and download the 802.1X client software.

After the host passes 802.1X authentication, the access device assigns the host to VLAN 5 where GigabitEthernet 2/0/3 is. The host can access the Internet.

Figure 40 Network diagram



Configuration procedure

1. Configure the 802.1X client. Make sure the 802.1X client can update its IP address after the access port is assigned to the guest VLAN or an authorization VLAN. (Details not shown.)
2. Configure the RADIUS server to provide authentication, authorization, and accounting services. Configure user accounts and authorization VLAN (VLAN 5 in this example) for the users. (Details not shown.)
3. Create VLANs, and assign ports to the VLANs on the access device.

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 2/0/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 2/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 2/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 2/0/3
[Device-vlan5] quit
```

4. Configure a RADIUS scheme on the access device:
 - # Create RADIUS scheme **2000** and enter RADIUS scheme view.
 - [Device] radius scheme 2000
 - # Specify the server at 10.11.1.1 as the primary authentication server, and set the authentication port to 1812.

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
# Specify the server at 10.11.1.1 as the primary accounting server, and set the accounting port to 1813.
[Device-radius-2000] primary accounting 10.11.1.1 1813
# Set the shared key to abc in plain text for secure communication between the authentication server and the device.
[Device-radius-2000] key authentication simple abc
# Set the shared key to abc in plain text for secure communication between the accounting server and the device.
[Device-radius-2000] key accounting simple abc
# Exclude the ISP domain names from the usernames sent to the RADIUS server.
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5. Configure an ISP domain:

```
# Create ISP domain bbb and enter ISP domain view.
[Device] domain bbb
# Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6. Configure 802.1X on the access device:

```
# Enable 802.1X on port GigabitEthernet 2/0/2.
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] dot1x
# Implement port-based access control on the port.
[Device-GigabitEthernet2/0/2] dot1x port-method portbased
# Set the port authorization mode to auto. By default, the port uses the auto mode.
[Device-GigabitEthernet2/0/2] dot1x port-control auto
# Specify VLAN 10 as the 802.1X guest VLAN on port GigabitEthernet 2/0/2.
[Device-GigabitEthernet2/0/2] dot1x guest-vlan 10
[Device-GigabitEthernet2/0/2] quit
# Enable 802.1X globally.
[Device] dot1x
```

Verifying the configuration

```
# Verify the 802.1X guest VLAN configuration on GigabitEthernet 2/0/2.
[Device] display dot1x interface gigabitethernet 2/0/2

# Verify that GigabitEthernet 2/0/2 is assigned to VLAN 10 before any user passes authentication on the port.
[Device] display vlan 10

# After a user passes authentication, display information on GigabitEthernet 2/0/2. Verify that GigabitEthernet 2/0/2 is assigned to VLAN 5.
[Device] display interface gigabitethernet 2/0/2
```

802.1X with ACL assignment configuration example

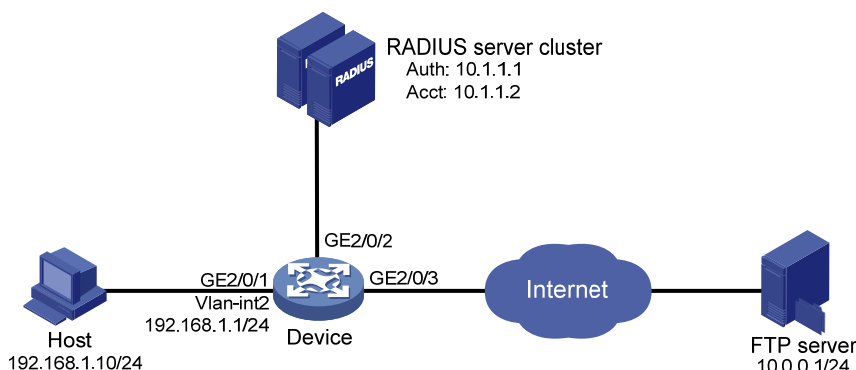
Network requirements

As shown in [Figure 41](#), the host that connects to GigabitEthernet 2/0/1 must pass 802.1X authentication to access the Internet.

Perform 802.1X authentication on GigabitEthernet 2/0/1. Use the RADIUS server at 10.1.1.1 as the authentication and authorization server, and the RADIUS server at 10.1.1.2 as the accounting server.

Configure ACL assignment on GigabitEthernet 2/0/1 to deny access of 802.1X users to the FTP server from 8:00 to 18:00 on weekdays.

Figure 41 Network diagram



Configuration procedure

1. Configure the 802.1X client. Make sure the client is able to update its IP address after the access port is assigned to the 802.1X guest VLAN or an authorization VLAN. (Details not shown.)
2. Configure the RADIUS servers to provide authentication, authorization, and accounting services. Add user accounts and specify the ACL (ACL 3000 in this example) for the users. (Details not shown.)
3. Assign an IP address to each interface, as shown in [Figure 41](#). (Details not shown.)
4. Configure a RADIUS scheme:
Create RADIUS scheme **2000** and enter RADIUS scheme view.

```
<Device> system-view
[Device] radius scheme 2000
```


Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```


Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```


Set the shared key to **abc** in plain text for secure communication between the authentication server and the device.

```
[Device-radius-2000] key authentication simple abc
```


Set the shared key to **abc** in plain text for secure communication between the accounting server and the device.

```
[Device-radius-2000] key accounting simple abc
```


Exclude the ISP domain names from the usernames sent to the RADIUS server.

- ```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```
5. Configure an ISP domain:
 

```
Create ISP domain bbb and enter ISP domain view.
[Device] domain bbb

Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```
  6. Configure a time range named **ftp** from 8:00 to 18:00 on weekdays.
 

```
[Device] time-range ftp 8:00 to 18:00 working-day
```
  7. Configure ACL 3000 to deny packets destined for the FTP server at 10.0.0.1 during the specified time range.
 

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-ipv4-adv-3000] quit
```
  8. Configure 802.1X:
 

```
Enable 802.1X on GigabitEthernet 2/0/1.
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] dot1x
[Device-GigabitEthernet2/0/1] quit

Enable 802.1X globally.
[Device] dot1x
```

### Verifying the configuration

- # Use the user account to pass authentication. (Details not shown.)
- # Verify that the user cannot ping the FTP server at any time from 8:00 to 18:00 on any weekday.

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 10.0.0.1:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The output shows that ACL 3000 is active on the user, and the user cannot access the FTP server.

## 802.1X with EAD assistant configuration example (with DHCP relay agent)

### Network requirements

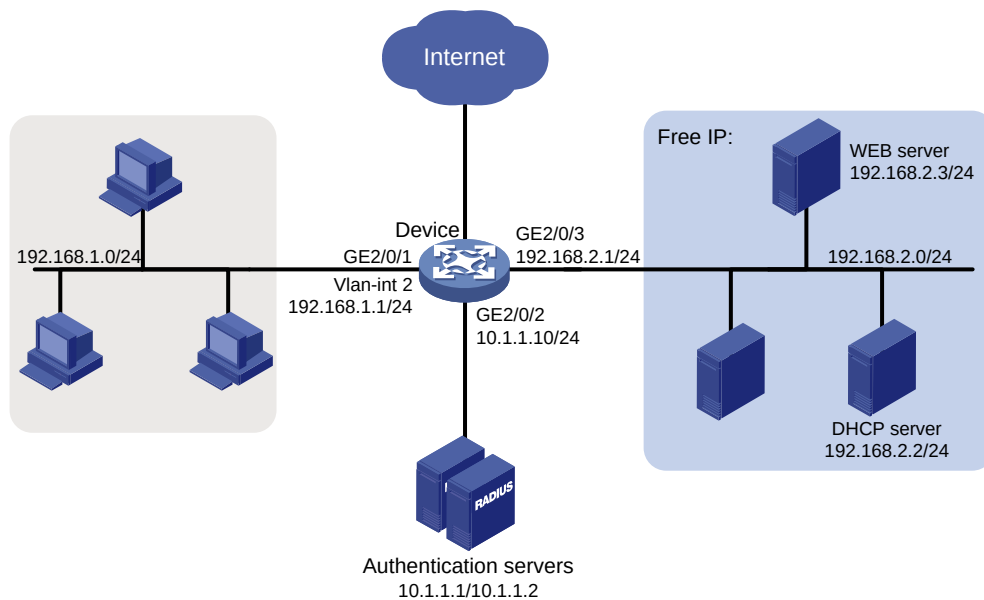
As shown in [Figure 42](#):

- The intranet 192.168.1.0/24 is attached to GigabitEthernet 2/0/1 of the access device.
- The hosts use DHCP to obtain IP addresses.
- A DHCP server and a Web server are deployed on the 192.168.2.0/24 subnet for users to obtain IP addresses and download client software.

Deploy an EAD solution for the intranet to meet the following requirements:

- Allow unauthenticated users and users who have failed 802.1X authentication to access 192.168.2.0/24. The users can obtain IP addresses and download software.
- If these users use a Web browser to access a network other than 192.168.2.0/24, redirect them to the Web server for 802.1X client downloading.
- Allow authenticated 802.1X users to access the network.

**Figure 42 Network diagram**



## Configuration procedure

1. Make sure the DHCP server, the Web server, and the authentication servers have been configured correctly. (Details not shown.)
2. Configure an IP address for each interface. (Details not shown.)
3. Configure DHCP relay:
  - # Enable DHCP.
  - ```
<Device> system-view
```
 - ```
[Device] dhcp enable
```
  - # Enable the DHCP relay agent on VLAN-interface 2.
  - ```
[Device] interface vlan-interface 2
```
 - ```
[Device-Vlan-interface2] dhcp select relay
```
  - # Specify the DHCP server 192.168.2.2 on the relay agent interface VLAN-interface 2.
  - ```
[Device-Vlan-interface2] dhcp relay server-address 192.168.2.2
```
 - ```
[Device-Vlan-interface2] quit
```
4. Configure a RADIUS scheme:
  - # Create RADIUS scheme **2000** and enter RADIUS scheme view.
  - ```
[Device] radius scheme 2000
```


Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```

Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```

Set the shared key to **abc** in plain text for secure communication between the authentication server and the device.

```
[Device-radius-2000] key authentication simple abc
```

Set the shared key to **abc** in plain text for secure communication between the accounting server and the device.

```
[Device-radius-2000] key accounting simple abc
```

Exclude the ISP domain names from the usernames sent to the RADIUS server.

```
[Device-radius-2000] user-name-format without-domain
```

```
[Device-radius-2000] quit
```

5. Configure an ISP domain:

Create ISP domain **bbb** and enter ISP domain view.

```
[Device] domain bbb
```

Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
```

```
[Device-isp-bbb] authorization lan-access radius-scheme 2000
```

```
[Device-isp-bbb] accounting lan-access radius-scheme 2000
```

```
[Device-isp-bbb] quit
```

6. Configure 802.1X:

Configure the free IP.

```
[Device] dot1x ead-assistant free-ip 192.168.2.0 24
```

Configure the redirect URL for client software download.

```
[Device] dot1x ead-assistant url http://192.168.2.3
```

Enable the EAD assistant feature.

```
[Device] dot1x ead-assistant enable
```

Enable 802.1X on GigabitEthernet 2/0/1.

```
[Device] interface gigabitethernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] dot1x
```

```
[Device-GigabitEthernet2/0/1] quit
```

Enable 802.1X globally.

```
[Device] dot1x
```

Verifying the configuration

Verify the 802.1X configuration.

```
[Device] display dot1x
```

Verify that you can ping an IP address on the free IP subnet from a host.

```
C:\>ping 192.168.2.3
```

Pinging 192.168.2.3 with 32 bytes of data:

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

The output shows that you can access the free IP subnet before passing 802.1X authentication.

Verify that you are redirected to the Web server when you enter in your Web browser an IP address not on the free IP. (Details not shown.)

802.1X with EAD assistant configuration example (with DHCP server)

Network requirements

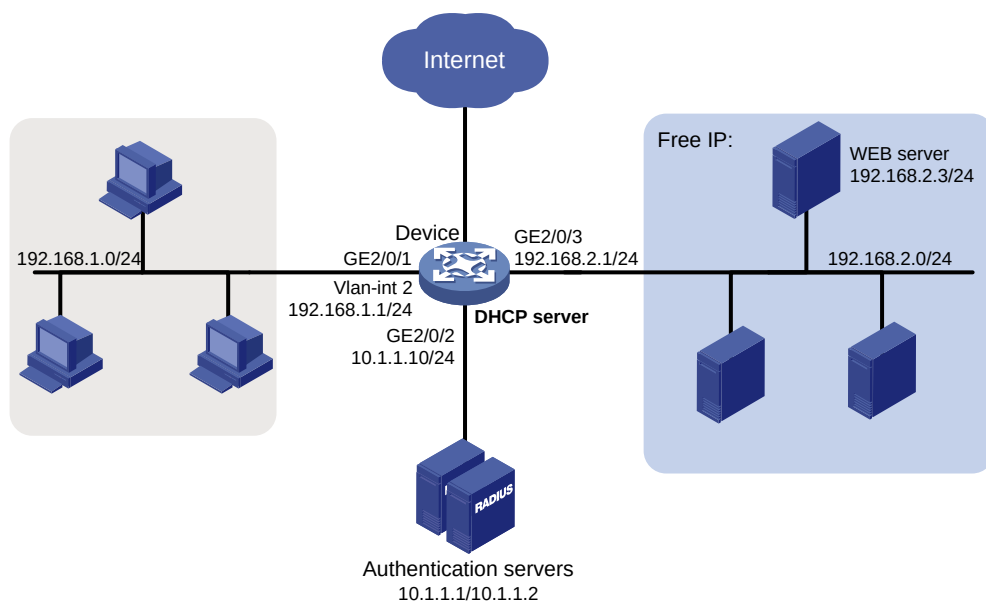
As shown in [Figure 43](#):

- The intranet 192.168.1.0/24 is attached to GigabitEthernet 2/0/1 of the access device.
- The hosts use DHCP to obtain IP addresses.
- A Web server is deployed on the 192.168.2.0/24 subnet for users to download client software.

Deploy an EAD solution for the intranet to meet the following requirements:

- Allow unauthenticated users and users who have failed 802.1X authentication to access 192.168.2.0/24. The users can download software.
- If these users use a Web browser to access a network other than 192.168.2.0/24, redirect them to the Web server for 802.1X client downloading.
- Allow authenticated 802.1X users to access the network.

Figure 43 Network diagram



Configuration procedure

1. Make sure the Web server and the authentication servers have been configured correctly. (Details not shown.)

2. Configure an IP address for each interface. (Details not shown.)
3. Configure the DHCP server:
 - # Enable DHCP.
 - <Device> system-view
 - [Device] dhcp enable
 - # Enable the DHCP server on VLAN-interface 2.
 - [Device] interface vlan-interface 2
 - [Device-Vlan-interface2] dhcp select server
 - [Device-Vlan-interface2] quit
 - # Create DHCP address pool 0.
 - [Device] dhcp server ip-pool 0
 - # Specify subnet 192.168.1.0/24 in DHCP address pool 0.
 - [Device-dhcp-pool-0] network 192.168.1.0 mask 255.255.255.0
 - # Specify the gateway address 192.168.1.1 in DHCP address pool 0.
 - [Device-dhcp-pool-0] gateway-list 192.168.1.1
 - [Device-dhcp-pool-0] quit
4. Configure a RADIUS scheme:
 - # Create RADIUS scheme **2000** and enter RADIUS scheme view.
 - [Device] radius scheme 2000
 - # Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.
 - [Device-radius-2000] primary authentication 10.1.1.1 1812
 - # Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.
 - [Device-radius-2000] primary accounting 10.1.1.2 1813
 - # Set the shared key to **abc** in plain text for secure communication between the authentication server and the device.
 - [Device-radius-2000] key authentication simple abc
 - # Set the shared key to **abc** in plain text for secure communication between the accounting server and the device.
 - [Device-radius-2000] key accounting simple abc
 - # Exclude the ISP domain names from the usernames sent to the RADIUS server.
 - [Device-radius-2000] user-name-format without-domain
 - [Device-radius-2000] quit
5. Configure an ISP domain:
 - # Create ISP domain **bbb** and enter ISP domain view.
 - [Device] domain bbb
 - # Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
 - [Device-isp-bbb] authentication lan-access radius-scheme 2000
 - [Device-isp-bbb] authorization lan-access radius-scheme 2000
 - [Device-isp-bbb] accounting lan-access radius-scheme 2000
 - [Device-isp-bbb] quit
6. Configure 802.1X:
 - # Configure the free IP.
 - [Device] dot1x ead-assistant free-ip 192.168.2.0 24
 - # Configure the redirect URL for client software download.

```
[Device] dot1x ead-assistant url http://192.168.2.3
# Enable the EAD assistant feature.
[Device] dot1x ead-assistant enable
# Enable 802.1X on GigabitEthernet 2/0/1.
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] dot1x
[Device-GigabitEthernet2/0/1] quit
# Enable 802.1X globally.
[Device] dot1x
```

Verifying the configuration

```
# Verify the 802.1X configuration.
[Device] display dot1x

# Verify that you can ping an IP address on the free IP subnet from a host.
C:\>ping 192.168.2.3
```

Pinging 192.168.2.3 with 32 bytes of data:

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The output shows that you can access the free IP subnet before passing 802.1X authentication.

Verify that you are redirected to the Web server when you enter in your Web browser an IP address not on the free IP. (Details not shown.)

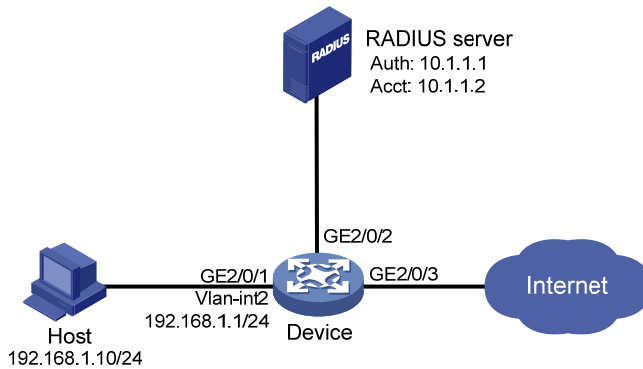
802.1X SmartOn configuration example

Network requirements

As shown in [Figure 44](#), configure the SmartOn feature on GigabitEthernet 2/0/1 so that the host must pass SmartOn authentication before 802.1X authentication.

Set the SmartOn password to **1234** in plain text and switch ID to **XYZ**. Set the SmartOn client timeout timer to 40 seconds.

Figure 44 Network diagram



Configuration procedure

1. Configure a RADIUS scheme:
 - # Create RADIUS scheme **2000** and enter RADIUS scheme view.
 - <Device> system-view
 - [Device] radius scheme 2000
 - # Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.
 - [Device-radius-2000] primary authentication 10.1.1.1 1812
 - # Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.
 - [Device-radius-2000] primary accounting 10.1.1.2 1813
 - # Set the shared key to **abc** in plain text for secure communication between the authentication server and the device.
 - [Device-radius-2000] key authentication simple abc
 - # Set the shared key to **abc** in plain text for secure communication between the accounting server and the device.
 - [Device-radius-2000] key accounting simple abc
 - # Exclude the ISP domain names from the usernames sent to the RADIUS server.
 - [Device-radius-2000] user-name-format without-domain
 - [Device-radius-2000] quit
2. Configure an ISP domain:
 - # Create ISP domain **bbb** and enter ISP domain view.
 - [Device] domain bbb
 - # Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
 - [Device-isp-bbb] authentication lan-access radius-scheme 2000
 - [Device-isp-bbb] authorization lan-access radius-scheme 2000
 - [Device-isp-bbb] accounting lan-access radius-scheme 2000
 - [Device-isp-bbb] quit
3. Configure 802.1X and SmartOn:
 - # Enable 802.1X on GigabitEthernet 2/0/1.
 - [Device] interface gigabitethernet 2/0/1
 - [Device-GigabitEthernet2/0/1] dot1x
 - # Enable SmartOn on GigabitEthernet 2/0/1.
 - [Device-GigabitEthernet2/0/1] dot1x smarton

```
[Device-GigabitEthernet2/0/1] quit
# Set the SmartOn password to 1234 in plain text and the switch ID to XYZ.
[Device] dot1x smarton password simple 1234
[Device] dot1x smarton switchid XYZ
# Set the SmartOn client timeout timer to 40 seconds.
[Device] smarton timer supp-timeout 40
# Enable 802.1X globally.
[Device] dot1x
```

Troubleshooting 802.1X

Web browser users cannot be redirected correctly

Symptom

Unauthenticated users are not redirected to the specified redirect URL after they enter external website addresses in their Web browsers.

Analysis

Redirection will not happen for one of the following reasons:

- The address is in the string format. The operating system of the host regards the string as a website name and tries to resolve the string. If the resolution fails, the operating system sends an ARP request, but the target address is not in the dotted decimal notation. The redirection feature does redirect this kind of ARP request.
- The address is within a free IP segment. No redirection will take place, even if no host is present with the address.
- The redirect URL is not in a free IP segment.
- No server is using the redirect URL, or the server with the URL does not provide Web services.

Solution

To resolve the problem:

1. Enter a dotted decimal IP address that is not in any free IP segments.
2. Verify that the access device and the server are configured correctly.
3. If the problem persists, contact Hewlett Packard Enterprise Support.

Configuring MAC authentication

Overview

MAC authentication controls network access by authenticating source MAC addresses on a port. The feature does not require client software, and users do not have to enter a username and password for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication-enabled port. If the MAC address passes authentication, the user can access authorized network resources. If the authentication fails, the device marks the MAC address as a silent MAC address, drops the packet, and starts a quiet timer. The device drops all subsequent packets from the MAC address within the quiet time. The quiet mechanism avoids repeated authentication during a short time.

NOTE:

If the MAC address that has failed authentication is a static MAC address or a MAC address that has passed any security authentication, the device does not mark the MAC address as a silent address.

User account policies

MAC authentication supports the following user account policies:

- One MAC-based user account for each user. The access device uses the source MAC addresses in packets as the usernames and passwords of users for MAC authentication. This policy is suitable for an insecure environment.
- One shared user account for all users. You specify one username and password, which are not necessarily a MAC address, for all MAC authentication users on the access device. This policy is suitable for a secure environment.

Authentication methods

You can perform MAC authentication on the access device (local authentication) or through a RADIUS server.

Local authentication:

- **MAC-based accounts**—The access device uses the source MAC address of the packet as the username and password to search the local account database for a match.
- **A shared account**—The access device uses the shared account username and password to search the local account database for a match.

RADIUS authentication:

- **MAC-based accounts**—The access device sends the source MAC address of the packet as the username and password to the RADIUS server for authentication.
- **A shared account**—The access device sends the shared account username and password to the RADIUS server for authentication.

For more information about configuring local authentication and RADIUS authentication, see "[Configuring AAA](#)."

VLAN assignment

You can specify the authorization VLAN for a MAC authentication user to control access to authorized network resources.

- On a RADIUS server, the authorization VLAN can be specified in the form of VLAN ID or VLAN name.
- On the local access device, the authorization VLAN must be specified in the form of VLAN ID. You can specify the authorization VLAN in the following views:
 - Local user view.
 - User group view.

For more information about local authorization VLAN configuration, see "[Configuring AAA](#)."

When the MAC authentication user passes authentication, the authentication server (either the local access device or a RADIUS server) assigns the authorization VLAN to the user.

The port through which the user accesses the device is assigned to the authorization VLAN. A hybrid port is always assigned to a server-assigned authorization VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

[Table 7](#) describes the way the network access device handles authorization VLANs for MAC authenticated users.

Table 7 VLAN manipulation

Port type	VLAN manipulation
• Access port • Trunk port • Hybrid port with MAC-based-VLAN disabled	The device assigns the first authenticated user's authorization VLAN to the port as the PVID. NOTE: For these port types, you must assign the same authorization VLAN to all MAC authentication users on a port. If a different authorization VLAN is assigned to a subsequent user, the user cannot pass MAC authentication.

ACL assignment

You can specify an authorization ACL in the user account for a MAC authentication user to control the user's access to network resources. After the user passes MAC authentication, the authentication server (local or remote) assigns the authorization ACL to the access port of the user. The ACL will filter traffic for this user. You must configure ACL rules for the authorization ACL on the access device for the ACL assignment feature.

To ensure a successful ACL assignment, make sure the ACL does not contain rules that match source MAC addresses.

To change the access control criteria for the user, you can use one of the following methods:

- Modify ACL rules on the access device.
- Specify another authorization ACL on the authentication server.

For more information about ACLs, see *ACL and QoS Configuration Guide*.

Periodic MAC reauthentication

Periodic MAC reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the RADIUS server. The attributes include the ACL and VLAN.

The device reauthenticates an online MAC authentication user periodically only after it receives the termination action **Radius-request** from the authentication server for this user. The Session-Timeout attribute (session timeout period) assigned by the server is the reauthentication interval. To display the server-assigned Session-Timeout and Termination-Action attributes, use the **display mac-authentication connection** command. Support for the server configuration and assignment of Session-Timeout and Termination-Action attributes depends on the server model.

When no server is reachable for MAC reauthentication, the device keeps the MAC authentication users online or logs off the users, depending on the keep-online feature configuration on the device. For information about the keep-online feature, see "[Configuring the keep-online feature](#)."

Compatibility information

Feature and hardware compatibility

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
 - HMIM-8GSW.
 - HMIM-24GSW.
 - HMIM-24GSWP
 - SIC-4GSW.
 - SIC-4GSWP.
- Fixed Layer 2 Ethernet ports on the following routers:
 - MSR954(JH296A/JH297A/JH298A/JH299A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Configuration prerequisites

Before you configure MAC authentication, complete the following tasks:

1. Configure an ISP domain and specify an AAA method. For more information, see "[Configuring AAA](#)."
 - For local authentication, you must also create local user accounts (including usernames and passwords), and specify the **lan-access** service for local users.
 - For RADIUS authentication, make sure the device and the RADIUS server can reach each other, and create user accounts on the RADIUS server. If you are using MAC-based accounts, make sure the username and password for each account are the same as the MAC address of each MAC authentication user.

2. Make sure the port security feature is disabled. For more information about port security, see "[Configuring port security](#)."

Configuration task list

Tasks at a glance
(Required.) Enabling MAC authentication
(Optional.) Specifying a MAC authentication domain
(Optional.) Configuring the user account format
(Optional.) Configuring MAC authentication timers
(Optional.) Setting the maximum number of concurrent MAC authentication users on a port
(Optional.) Configuring MAC authentication delay
(Optional.) Enabling MAC authentication multi-VLAN mode on a port
(Optional.) Configuring the keep-online feature

Enabling MAC authentication

For MAC authentication to take effect on a port, you must enable this feature globally and on the port. MAC authentication is exclusive with link aggregation group.

- You cannot enable MAC authentication on a port already in a link aggregation group.
- You cannot add a MAC authentication-enabled port to a link aggregation group.

To enable MAC authentication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MAC authentication globally.	mac-authentication	By default, MAC authentication is disabled globally.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable MAC authentication on the port.	mac-authentication	By default, MAC authentication is disabled on a port.

Specifying a MAC authentication domain

By default, MAC authentication users are in the system default authentication domain. To implement different access policies for users, you can use one of the following methods to specify authentication domains for MAC authentication users:

- Specify a global authentication domain in system view. This domain setting applies to all ports enabled with MAC authentication.
- Specify an authentication domain for an individual port in interface view.

MAC authentication chooses an authentication domain for users on a port in this order: the port-specific domain, the global domain, and the default domain. For more information about authentication domains, see "[Configuring AAA](#)."

To specify an authentication domain for MAC authentication users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify an authentication domain for MAC authentication users.	- In system view: mac-authentication domain <i>domain-name</i> - In Layer 2 Ethernet interface view: a. interface <i>interface-type</i> <i>interface-number</i> b. mac-authentication domain <i>domain-name</i>	By default, the system default authentication domain is used for MAC authentication users.

Configuring the user account format

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the MAC authentication user account format.	- Use one MAC-based user account for each user: mac-authentication user-name-format <i>mac-address</i> [{ with-hyphen without-hyphen }] [lowercase uppercase]] - Use one shared user account for all users: mac-authentication user-name-format fixed [account <i>name</i>] [password { cipher simple } <i>password</i>]	By default, the device uses the MAC address of a user as the username and password for MAC authentication. The MAC address is in the hexadecimal notation without hyphens, and letters are in lower case.

Configuring MAC authentication timers

MAC authentication uses the following timers:

- Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device regards the user idle. If a user connection has been idle within the interval, the device logs the user out and stops accounting for the user.
- Quiet timer**—Sets the interval that the device must wait before the device can perform MAC authentication for a user who has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before the device regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

To configure MAC authentication timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Configure MAC authentication timers.	mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> }	By default, the offline detect timer is 300 seconds, the quiet timer is 60 seconds, and the server timeout timer is 100 seconds.

Setting the maximum number of concurrent MAC authentication users on a port

Perform this task to prevent the system resources from being overused.

To set the maximum number of concurrent MAC authentication users on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the maximum number of concurrent MAC authentication users on the port	mac-authentication max-user <i>user-number</i>	The default setting is 4096.

Configuring MAC authentication delay

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered.

If no 802.1X authentication is triggered or 802.1X authentication fails within the delay period, the port continues to process MAC authentication.

Do not set the port security mode to **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** when you use MAC authentication delay. The delay does not take effect on a port in either of the two modes. For more information about port security modes, see "[Configuring port security](#)."

To configure MAC authentication delay:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable MAC authentication delay and set the delay timer.	mac-authentication timer auth-delay <i>time</i>	By default, MAC authentication delay is disabled.

Enabling MAC authentication multi-VLAN mode on a port

The MAC authentication multi-VLAN mode prevents an authenticated online user from service interruption caused by VLAN changes on a port. When the port receives a packet sourced from the user in a VLAN not matching the existing MAC-VLAN mapping, the device neither logs off the user nor reauthenticates the user. The device creates a new MAC-VLAN mapping for the user, and traffic transmission is not interrupted. The original MAC-VLAN mapping for the user remains on the device until it dynamically ages out. As a best practice, configure this feature on hybrid or trunk ports.

This feature improves transmission of data that is vulnerable to delay and interference. It is typically applicable to IP phone users.

To enable MAC authentication multi-VLAN mode on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable MAC authentication multi-VLAN mode.	mac-authentication host-mode multi-vlan	By default, this feature is disabled on a port. When the port receives a packet sourced from an authenticated user in a VLAN not matching the existing MAC-VLAN mapping, the device logs off and reauthenticates the user.

Configuring the keep-online feature

By default, the device logs off online MAC authentication users if no server is reachable for MAC reauthentication. The keep-online feature keeps authenticated MAC authentication users online when no server is reachable for MAC reauthentication.

In a fast-recovery network, you can use the keep-online feature to prevent MAC authentication users from coming online and going offline frequently.

To configure the keep-online feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the keep-online feature for authenticated MAC authentication users on the port.	mac-authentication re-authenticate server-unreachable keep-online	By default, the keep-online feature is disabled. This command takes effect only when the authentication server assigns reauthentication attributes to the device.

Displaying and maintaining MAC authentication

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display MAC authentication information.	display mac-authentication [interface <i>interface-type interface-number</i>]
Display MAC authentication connections (centralized devices in standalone mode).	display mac-authentication connection [interface <i>interface-type interface-number</i> user-mac <i>mac-addr</i> user-name <i>user-name</i>]
Display MAC authentication connections (distributed devices in standalone mode/centralized devices in IRF mode).	display mac-authentication connection [interface <i>interface-type interface-number</i> slot <i>slot-number</i> user-mac <i>mac-addr</i> user-name <i>user-name</i>]
Display MAC authentication connections (distributed devices in IRF mode).	display mac-authentication connection [chassis <i>chassis-number</i> slot <i>slot-number</i> interface <i>interface-type interface-number</i> user-mac <i>mac-addr</i> user-name <i>user-name</i>]
Clear MAC authentication statistics.	reset mac-authentication statistics [interface <i>interface-type interface-number</i>]

MAC authentication configuration examples

Local MAC authentication configuration example

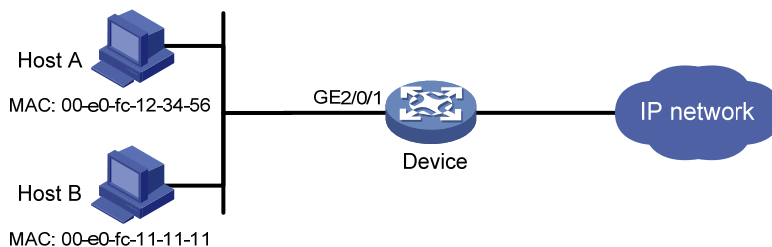
Network requirements

As shown in Figure 45, the device performs local MAC authentication on port GigabitEthernet 2/0/1 to control Internet access of users.

Configure the device to meet the following requirements:

- Detect whether a user has gone offline every 180 seconds.
- Deny a user for 180 seconds if the user fails MAC authentication.
- Authenticate all users in ISP domain **bbb**.
- Use the MAC address of each user as the username and password for authentication. A MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.

Figure 45 Network diagram



Configuration procedure

Add a network access local user. In this example, configure both the username and password as Host A's MAC address 00-e0-fc-12-34-56.

```
<Device> system-view
```

```

[Device] local-user 00-e0-fc-12-34-56 class network
[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
# Specify the LAN access service for the user.
[Device-luser-network-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-network-00-e0-fc-12-34-56] quit
# Configure ISP domain bbb to perform local authentication for LAN users.
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
# Enable MAC authentication on port GigabitEthernet 2/0/1.
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] mac-authentication
[Device-GigabitEthernet2/0/1] quit
# Specify the MAC authentication domain as the ISP domain bbb.
[Device] mac-authentication domain bbb
# Configure MAC authentication timers.
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
# Configure MAC authentication to use MAC-based accounts. Each MAC address is in the
hexadecimal notation with hyphens, and letters are in lower case.
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
# Enable MAC authentication globally.
[Device] mac-authentication

```

Verifying the configuration

```

# Display MAC authentication settings and statistics to verify your configuration.
[Device] display mac-authentication
Global MAC authentication parameters:
    MAC authentication      : Enabled
    User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
        Username          : mac
        Password          : Not configured
    Offline detect period  : 180 s
    Quiet period           : 180 s
    Server timeout         : 100 s
    Authentication domain  : bbb
Max MAC-auth users       : 1024 per slot
Online MAC-auth users    : 1

Silent MAC users:
    MAC address      VLAN ID  From port          Port index
    00e0-fc11-1111   8      GigabitEthernet2/0/1  1
GigabitEthernet2/0/1 is link-up
    MAC authentication      : Enabled
    Authentication domain   : Not configured
    Auth-delay timer        : Disabled
    Re-auth server-unreachable : Logoff

```

```

Host mode                : Single VLAN
Max online users          : 4096
Authentication attempts   : successful 1, failed 0
Current online users      : 1

      MAC address      Auth state
      00e0-fc12-3456   Authenticated

```

The output shows that Host A has passed MAC authentication and has come online. Host B failed MAC authentication and its MAC address is marked as a silent MAC address.

RADIUS-based MAC authentication configuration example

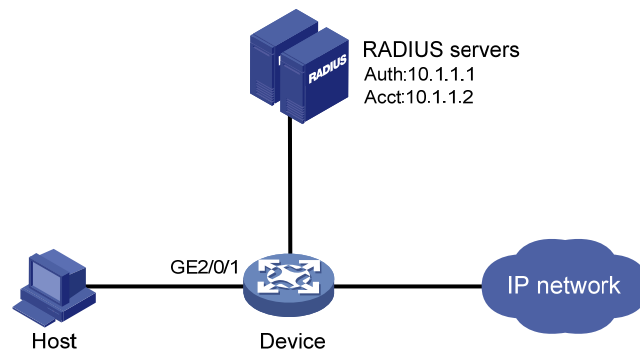
Network requirements

As shown in [Figure 46](#), the device uses RADIUS servers to perform authentication, authorization, and accounting for users.

To control user access to the Internet by MAC authentication, perform the following tasks:

- Enable MAC authentication globally and on port GigabitEthernet 2/0/1.
- Configure the device to detect whether a user has gone offline every 180 seconds.
- Configure the device to deny a user for 180 seconds if the user fails MAC authentication.
- Configure all users to belong to the ISP domain **bbb**.
- Use a shared user account for all users, with the username **aaa** and password **123456**.

Figure 46 Network diagram



Configuration procedure

1. Make sure the RADIUS server and the access device can reach each other. (Details not shown.)
2. Configure the RADIUS servers:
 - # Create a shared account for MAC authentication users. (Details not shown.)
 - # Set the username **aaa** and password **123456** for the account. (Details not shown.)
3. Configure RADIUS-based MAC authentication on the device:
 - # Configure a RADIUS scheme.

```

<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc

```



```

[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
# Apply the RADIUS scheme to ISP domain bbb for authentication, authorization, and
accounting.
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
# Enable MAC authentication on port GigabitEthernet 2/0/1.
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] mac-authentication
[Device-GigabitEthernet2/0/1] quit
# Specify the MAC authentication domain as the ISP domain bbb.
[Device] mac-authentication domain bbb
# Set MAC authentication timers.
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
# Specify username aaa and password 123456 in plain text for the account shared by MAC
authentication users.
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
# Enable MAC authentication globally.
[Device] mac-authentication

```

Verifying the configuration

Verify the MAC authentication configuration.

```
[Device] display mac-authentication
```

Global MAC authentication parameters:

```

MAC authentication      : Enabled
User name format       : Fixed account
    Username           : aaa
    Password           : *****
Offline detect period   : 180 s
Quiet period           : 180 s
Server timeout         : 100 s
Authentication domain   : bbb
Max MAC-auth users     : 1024 per slot
Online MAC-auth users   : 1

```

Silent MAC users:

MAC address	VLAN ID	From port	Port index

GigabitEthernet2/0/1 is link-up

```

MAC authentication      : Enabled
Authentication domain    : Not configured
Auth-delay timer        : Disabled
Re-auth server-unreachable : Logoff
Host mode               : Single VLAN
Max online users         : 4096

```

```

Authentication attempts    : successful 1, failed 0
Current online users       : 1
      MAC address          Auth state
      00e0-fc12-3456      Authenticated

```

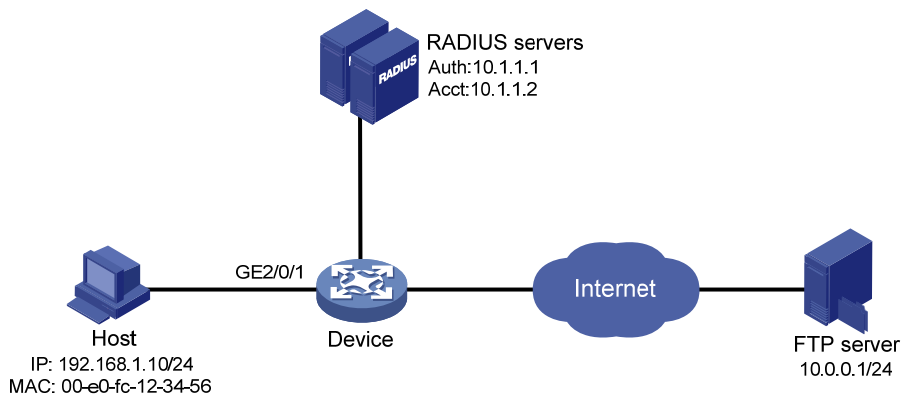
ACL assignment configuration example

Network requirements

As shown in [Figure 47](#), configure the device to meet the following requirements:

- Use RADIUS servers to perform authentication, authorization, and accounting for users.
- Perform MAC authentication on port GigabitEthernet 2/0/1 to control Internet access.
- Use MAC-based user accounts for MAC authentication users. Each MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.
- Use an ACL to deny authenticated users to access the FTP server at 10.0.0.1.

Figure 47 Network diagram



Configuration procedure

Make sure the RADIUS servers and the access device can reach each other.

1. Configure ACL 3000 to deny packets destined for 10.0.0.1.

```

<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Sysname-acl-ipv4-adv-3000] quit

```

2. Configure RADIUS-based MAC authentication on the device:

Configure a RADIUS scheme.

```

[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.1.1.1 1812
[Sysname-radius-2000] primary accounting 10.1.1.2 1813
[Sysname-radius-2000] key authentication simple abc
[Sysname-radius-2000] key accounting simple abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit

```

Apply the RADIUS scheme to an ISP domain for authentication, authorization, and accounting.

```

[Sysname] domain bbb
[Sysname-isp-bbb] authentication default radius-scheme 2000

```

```
[Sysname-isp-bbb] authorization default radius-scheme 2000
[Sysname-isp-bbb] accounting default radius-scheme 2000
[Sysname-isp-bbb] quit
# Specify the ISP domain for MAC authentication.
[Sysname] mac-authentication domain bbb
# Configure the device to use MAC-based user accounts. Each MAC address is in the
hexadecimal notation with hyphens, and letters are in lower case.
[Sysname] mac-authentication user-name-format mac-address with-hyphen lowercase
# Enable MAC authentication on port GigabitEthernet 2/0/1.
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] mac-authentication
[Sysname-GigabitEthernet2/0/1] quit
# Enable MAC authentication globally.
[Sysname] mac-authentication
```

3. Configure the RADIUS servers:

```
# Add a user account with 00-e0-fc-12-34-56 as both the username and password on each
RADIUS server. (Details not shown.)
# Specify ACL 3000 as the authorization ACL for the user account. (Details not shown.)
```

Verifying the configuration

```
# Verify the MAC authentication configuration.
[Sysname] display mac-authentication
Global MAC authentication parameters:
    MAC authentication      : Enabled
    User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
        Username           : mac
        Password           : Not configured
    Offline detect period  : 180 s
    Quiet period           : 180 s
    Server timeout         : 100 s
    Authentication domain  : bbb
    Max MAC-auth users     : 1024 per slot
    Online MAC-auth users  : 2
```

Silent MAC users:

MAC address	VLAN ID	From port	Port index

```
GigabitEthernet2/0/1 is link-up
    MAC authentication      : Enabled
    Authentication domain   : Not configured
    Auth-delay timer        : Disabled
    Re-auth server-unreachable : Logoff
    Host mode               : Single VLAN
    Max online users        : 4096
    Authentication attempts : successful 1, failed 0
    Current online users    : 1
        MAC address        Auth state
        00e0-fc12-3456     Authenticated
```

Verify that you cannot ping the FTP server from the host.

```
C:\>ping 10.0.0.1
```

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 10.0.0.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

The output shows that ACL 3000 has been assigned to port GigabitEthernet 2/0/1 to deny access to the FTP server.

Configuring portal authentication

Overview

Portal authentication controls user access to the Internet. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication. When portal authentication is deployed on a network, an access device redirects unauthenticated users to the website provided by a portal Web server. The users can access the resources on the website without authentication. If the users want to access the Internet, they must pass authentication on the website.

Portal authentication is classified into the following types:

- **Active authentication**—Users visit the authentication website provided by the portal Web server and enter their username and password for authentication.
- **Forced authentication**—Users are redirected to the portal authentication website for authentication when they visit other websites.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Allows users to perform authentication through Web pages without installing client software.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.
- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assignment scheme and saves public IP addresses. Cross-subnet authentication can authenticate users who reside in a different subnet than the access device.

The device supports Portal 1.0, Portal 2.0, and Portal 3.0.

Extended portal functions

By forcing patching and anti-virus policies, extended portal functions help hosts to defend against viruses. Portal supports the following extended functions:

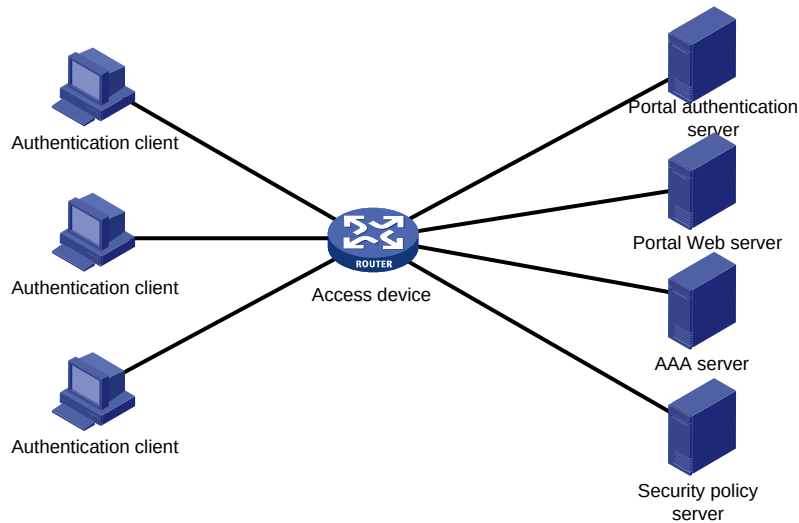
- **Security check**—Detects after authentication whether or not a user host installs anti-virus software, virus definition file, unauthorized software, and operating system patches.
- **Resource access restriction**—Allows an authenticated user to access certain network resources such as the virus server and the patch server. Users can access more Internet resources after passing security check.

Security check must cooperate with the HPE IMC security policy server and the iNode client.

Portal system components

A typical portal system consists of these basic components: authentication client, access device, portal authentication server, portal Web server, AAA server, and security policy server.

Figure 48 Portal system components



Authentication client

An authentication client is a Web browser that runs HTTP/HTTPS or a user host that runs a portal client application. Security check for the user host is implemented through the interaction between the portal client and the security policy server.

Access device

An access device refers to a broadband access device such as a switch or a router. An access device has the following functions:

- Redirects all HTTP requests of unauthenticated users to the portal Web server.
- Interacts with the portal authentication server and the AAA server to complete authentication, authorization, and accounting.
- Allows users that pass portal authentication to access authorized Internet resources.

Portal authentication server

The portal authentication server receives authentication requests from authentication clients and interacts with the access device to authenticate users.

Portal Web server

The portal Web server pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server. The access device also redirects HTTP requests from unauthenticated users to the portal Web server.

The portal Web server can be integrated with the portal authentication server or an independent server.

AAA server

The AAA server interacts with the access device to implement authentication, authorization, accounting for portal users. In a portal system, a RADIUS server can perform authentication, authorization, accounting for portal users, and an LDAP server can perform authentication for portal users.

Security policy server

The security policy server interacts with the portal client and the access device for security check and authorization for users.

Interaction between portal system components

The components of a portal system interact as follows:

1. An unauthenticated user initiates authentication by accessing an Internet website through a Web browser. When receiving the HTTP request, the access device redirects it to the Web authentication page provided by the portal Web server. The user can also visit the authentication website to log in. The user must log in through the HPE iNode client for extended portal functions.
2. The user enters the authentication information on the authentication page/dialog box and submits the information. The portal Web server forwards the information to the portal authentication server. Then the portal authentication server processes the information and forwards it to the access device.
3. The access device interacts with the AAA server to implement authentication, authorization, accounting for the user.
4. If security policies are not imposed on the user, the access device allows the authenticated user to access the Internet. If security policies are imposed on the user, the portal client, the access device, and the security policy server interact to check the user host. If the user passes the security check, the security policy server authorizes the user to access resources based on the check result. Portal authentication through Web does not support security check for users. To implement security check, the client must be the HPE iNode client.

NOTE:

Portal authentication supports NAT traversal whether it is initiated by a Web client or an HPE iNode client. When the portal authentication client is on a private network, the portal authentication server is on a public network, and the access device is enabled with NAT, network address translations performed on the access device do not affect portal authentication. As a best practice, use an interface's public IP address as the source address of outgoing portal packets.

Portal authentication modes

Portal authentication has three modes: direct authentication, re-DHCP authentication, and cross-subnet authentication. In direct authentication and re-DHCP authentication, no Layer 3 forwarding devices exist between the authentication client and the access device. In cross-subnet authentication, Layer 3 forwarding devices can exist between the authentication client and the access device.

Direct authentication

A user manually configures a public IP address or obtains a public IP address through DHCP. Before authentication, the user can access only the portal Web server and predefined authentication-free websites. After passing authentication, the user can access other network resources. The process of direct authentication is simpler than that of re-DHCP authentication.

Re-DHCP authentication

Before a user passes authentication, DHCP allocates an IP address (a private IP address) to the user. The user can access only the portal Web server and predefined authentication-free websites. After the user passes authentication, DHCP reallocates an IP address (a public IP address) to the user. The user then can access other network resources. No public IP address is allocated to users who fail authentication. Re-DHCP authentication saves public IP addresses. For example, an ISP can allocate public IP addresses to broadband users only when they access networks beyond the residential community network.

Only the HPE iNode client supports re-DHCP authentication. IPv6 portal authentication does not support the re-DHCP authentication mode.

Cross-subnet authentication

Cross-subnet authentication is similar to direct authentication, except it allows Layer 3 forwarding devices to exist between the authentication client and the access device.

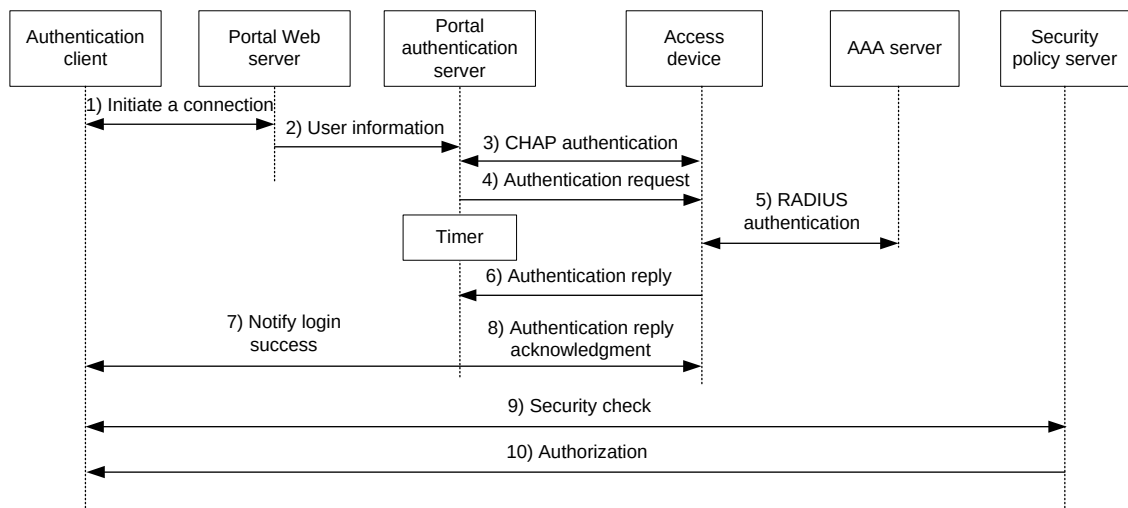
In direct authentication, re-DHCP authentication, and cross-subnet authentication, a user's IP address uniquely identifies the user. After a user passes authentication, the access device generates an ACL for the user based on the user's IP address to control forwarding of the packets from the user. Because no Layer 3 forwarding device exists between authentication clients and the access device in direct authentication and re-DHCP authentication, the access device can learn the user MAC addresses. The access device can enhance its capability of controlling packet forwarding by using the learned MAC addresses.

Portal authentication process

Direct authentication and cross-subnet authentication share the same authentication process. Re-DHCP authentication has a different process as it has two address allocation procedures.

Direct authentication/cross-subnet authentication process (with CHAP/PAP authentication)

Figure 49 Direct authentication/cross-subnet authentication process



The direct/cross-subnet authentication process is as follows:

1. A portal user access the Internet through HTTP, and the HTTP packet arrives at the access device.
 - If the packet matches a portal free rule, the access device allows the packet to pass.
 - If the packet does not match any portal-free rule, the access device redirects the packet to the portal Web server. The portal Web server pushes the Web authentication page to the user for him to enter his username and password.
2. The portal Web server submits the user authentication information to the portal authentication server.
3. The portal authentication server and the access device exchange CHAP messages. This step is skipped for PAP authentication. The portal authentication server decides the method (CHAP or PAP) to use.
4. The portal authentication server adds the username and password into an authentication request packet and sends it to the access device. Meanwhile, the portal authentication server starts a timer to wait for an authentication reply packet.
5. The access device and the RADIUS server exchange RADIUS packets.

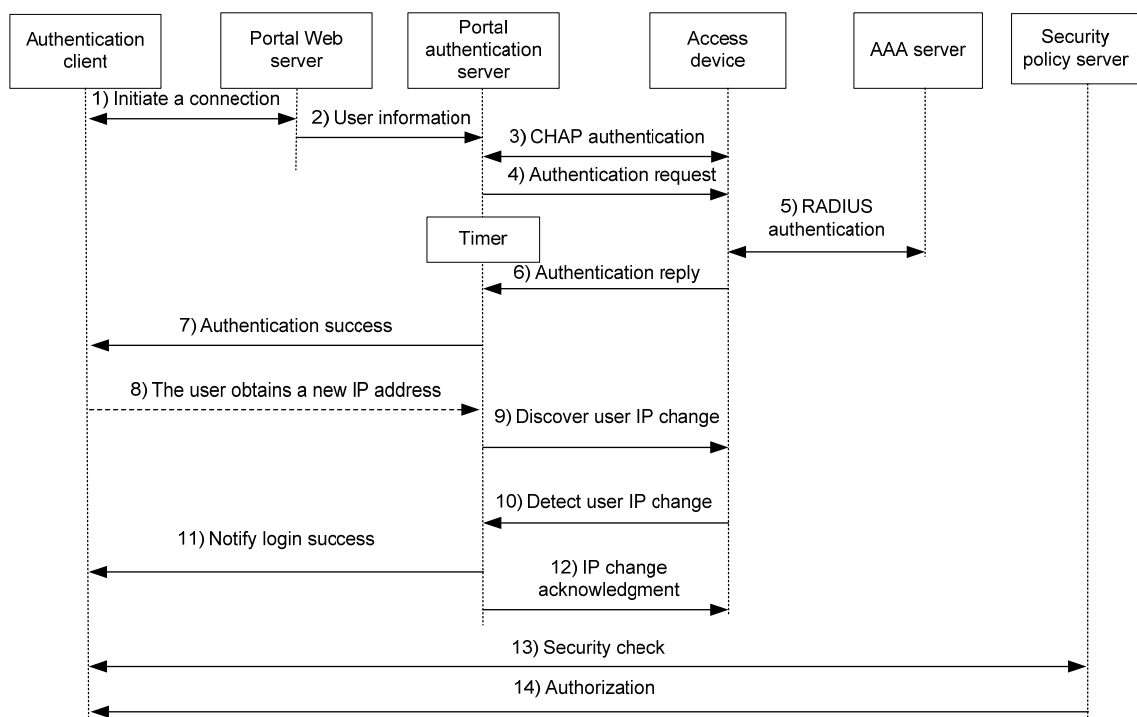
6. The access device sends an authentication reply packet to the portal authentication server to notify authentication success or failure.
7. The portal authentication server sends an authentication success or failure packet to the client.
8. If the authentication is successful, the portal authentication server sends an authentication reply acknowledgment packet to the access device.

If the client is an iNode client, the authentication process includes step 9 and step 10 for extended portal functions. Otherwise the authentication process is complete.

9. The client and the security policy server exchange security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.
10. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.

Re-DHCP authentication process (with CHAP/PAP authentication)

Figure 50 Re-DHCP authentication process



The re-DHCP authentication process is as follows:

Step 1 through step 7 are the same as those in the direct authentication/cross-subnet authentication process.

8. After receiving the authentication success packet, the client obtains a public IP address through DHCP. The client then notifies the portal authentication server that it has a public IP address.
9. The portal authentication server notifies the access device that the client has obtained a public IP address.
10. The access device detects the IP change of the client through DHCP and then notifies the portal authentication server that it has detected an IP change of the client IP.
11. After receiving the IP change notification packets sent by the client and the access device, the portal authentication server notifies the client of login success.
12. The portal authentication server sends an IP change acknowledgment packet to the access device.

Step 13 and step 14 are for extended portal functions.

13. The client and the security policy server exchanges security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.
14. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.

Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Portal configuration task list

Tasks at a glance
(Required.) Configuring a portal authentication server
(Required.) Configuring a portal Web server
(Required.) Enabling portal authentication on an interface
(Required.) Referencing a portal Web server for an interface
(Optional.) Controlling portal user access • Configuring a portal-free rule • Configuring an authentication source subnet • Configuring an authentication destination subnet • Setting the maximum number of portal users • Specifying a portal authentication domain • Specifying a preauthentication domain • Configuring a preauthentication IP address pool for portal users • Enabling strict-checking on portal authorization information • Enabling outgoing packets filtering on a portal-enabled interface
(Optional.) Configuring portal detection features • Configuring online detection of portal users • Configuring portal authentication server detection • Configuring portal Web server detection • Configuring portal user synchronization
(Optional.) Configuring the portal fail-permit feature
(Optional.) Configuring BAS-IP for portal packets sent to the portal authentication server
(Optional.) Enabling portal roaming
(Optional.) Specifying a format for the NAS-Port-ID attribute

Tasks at a glance
(Optional.) Logging out portal users
(Optional.) Configuring Web redirect On Etherchannel interfaces, both Web redirect and portal authentication can be enabled at the same time. On other types of interfaces, Web redirect does not work when both Web redirect and portal authentication are enabled.
(Optional.) Applying a NAS-ID profile to an interface

Configuration prerequisites

The portal feature provides a solution for user identity authentication and security check. To complete user identity authentication, portal must cooperate with RADIUS.

The prerequisites for portal authentication configuration are as follows:

- The portal authentication server, portal Web server, and RADIUS server have been installed and configured correctly.
- To use the re-DHCP portal authentication mode, make sure the DHCP relay agent is enabled on the access device, and the DHCP server is installed and configured correctly.
- The portal client, access device, and servers can reach each other.
- To use the remote RADIUS server, configure usernames and passwords on the RADIUS server, and configure the RADIUS client on the access device. For information about RADIUS client configuration, see "[Configuring AAA](#)."
- To implement extended portal functions, install and configure IMC EAD. Make sure the ACLs configured on the access device correspond to the isolation ACL and the security ACL on the security policy server. For information about security policy server configuration on the access device, see "[Configuring AAA](#)." For installation and configuration about the security policy server, see *IMC EAD Security Policy Help*.

Configuring a portal authentication server

Perform this task to configure the following portal authentication server parameters:

- IP address of the portal authentication server
- VPN instance of the portal authentication server
- Shared encryption key used between the device and the portal authentication server
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server

The device supports multiple portal authentication servers.

Do not delete a portal authentication server in use. Otherwise, users authenticated by that server cannot log out normally.

To configure a portal authentication server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a portal authentication server, and enter its view.	portal server <i>server-name</i>	By default, no portal authentication server is created.

Step	Command	Remarks
3. Specify the IP address of the portal authentication server.	- To specify an IPv4 portal server: ip <i>ipv4-address</i> [vpn-instance <i>vpn-instance-name</i>] [key { cipher simple } <i>key-string</i>] - To specify an IPv6 portal server: ipv6 <i>ipv6-address</i> [vpn-instance <i>vpn-instance-name</i>] [key { cipher simple } <i>key-string</i>]	Specify an IPv4 portal authentication server, an IPv6 authentication portal server, or both. By default, no portal authentication server is specified.
4. (Optional.) Set the destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.	port <i>port-id</i>	By default, the UDP port number is 50100. This port number must be the same as the listening port number specified on the portal authentication server.

Configuring a portal Web server

Perform this task to configure the following portal Web server parameters:

- VPN instance of the portal Web server
- URL of the portal Web server
- Parameters carried in the URL when the device redirects the URL to users

The device supports multiple portal Web servers.

To configure a portal Web server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a portal Web server and enter its view.	portal web-server <i>server-name</i>	By default, no portal Web server is created.
3. Specify the VPN instance to which the portal Web server belongs.	vpn-instance <i>vpn-instance-name</i>	By default, the portal Web server belongs to the public network.
4. Specify the URL of the portal Web server.	url <i>url-string</i>	By default, no URL is specified.
5. Configure the parameters to be carried in the URL when the device redirects it to users.	url-parameter <i>param-name</i> { original-uri source-address source-mac value <i>expression</i> }	By default, no redirection URL parameters are configured.

Enabling portal authentication on an interface

You must first enable portal authentication on an access interface before it can perform portal authentication for connected clients.

When a portal-enabled interface receives a portal packet, it checks the source IP address and VPN information of the packet. If the packet matches a locally configured portal authentication server, the interface regards the packet valid and sends an authentication response packet to the portal authentication server. Otherwise, the interface drops the packet. After a user logs in to the device, the user interacts with the portal authentication server as needed.

Configuration restrictions and guidelines

When you enable portal authentication on an interface, follow these restrictions and guidelines:

- Make sure the interface has a valid IP address before you enable re-DHCP portal authentication on the interface.
- Do not add the Ethernet interface enabled with portal authentication to an aggregation group. Otherwise, portal authentication does not take effect.
- Cross-subnet authentication mode (**layer3**) does not require Layer 3 forwarding devices between the access device and the portal authentication clients. However, if a Layer 3 forwarding device exists between the authentication client and the access device, you must use the cross-subnet portal authentication mode.
- With re-DHCP portal authentication, configure authorized ARP on the interface as a best practice to make sure only valid users can access the network. With authorized ARP configured on the interface, the interface learns ARP entries only from the users who have obtained a public address from DHCP.
- For successful re-DHCP portal authentication, make sure the BAS-IP/BAS-IPv6 attribute value is the same as the device IP or IPv6 address specified on the portal authentication server. To configure the BAS-IP/BAS-IPv6 attribute, use the **portal { bas-ip | bas-ipv6 }** command.
- An IPv6 portal server does not support the re-DHCP portal authentication mode.
- You can enable both IPv4 portal authentication and IPv6 portal authentication on an interface.

Configuration procedure

To enable portal authentication on an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	The interface must be a Layer 3 interface.
3. Enable portal authentication on the interface.	• To enable IPv4 portal authentication: portal enable method { direct layer3 redhcp } • To enable IPv6 portal authentication: portal ipv6 enable method { direct layer3 }	Enable IPv4 portal authentication, IPv6 portal authentication, or both on the interface.

Referencing a portal Web server for an interface

After you reference a portal Web server for an interface, the device redirects the HTTP requests of the portal users on the interface to the portal Web server.

An interface can reference both an IPv4 portal Web server and an IPv6 portal Web server.

To reference a portal Web server for an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	The interface must be a Layer 3 interface.

Step	Command	Remarks
3. Reference a portal Web server for the interface.	- To reference an IPv4 portal Web server: portal apply web-server <i>server-name</i> [fail-permit] - To reference an IPv6 portal Web server: portal ipv6 apply web-server <i>server-name</i> [fail-permit]	Reference an IPv4 portal Web server, an IPv6 portal Web server, or both for the interface. By default, the interface does not reference any portal Web server.

Controlling portal user access

Configuring a portal-free rule

A portal-free rule allows specified users to access specified external websites without portal authentication.

The matching items for a portal-free rule include the source/destination IP address, TCP/UDP port number, source MAC address, access interface, and VLAN. Packets matching a portal-free rule will not trigger portal authentication, so users sending the packets can directly access the specified external websites.

You cannot configure two or more portal-free rules with the same filtering criteria. Otherwise, the system prompts that the rule already exists.

Regardless of whether portal authentication is enabled or not, you can only add or remove a portal-free rule. You cannot modify it.

To configure an IP-based portal-free rule:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure an IPv4-based portal-free rule.	portal free-rule <i>rule-number</i> { destination ip { <i>ip-address</i> { <i>mask-length</i> <i>mask</i> } any } [tcp <i>tcp-port-number</i> udp <i>udp-port-number</i>] source ip { <i>ip-address</i> { <i>mask-length</i> <i>mask</i> } any } [tcp <i>tcp-port-number</i> udp <i>udp-port-number</i>] } * [interface <i>interface-type interface-number</i>]	By default, no IPv4-based portal-free rule exists.
3. Configure an IPv6-based portal-free rule.	portal free-rule <i>rule-number</i> { destination ipv6 { <i>ipv6-address</i> <i>prefix-length</i> any } [tcp <i>tcp-port-number</i> udp <i>udp-port-number</i>] source ipv6 { <i>ipv6-address</i> <i>prefix-length</i> any } [tcp <i>tcp-port-number</i> udp <i>udp-port-number</i>] } * [interface <i>interface-type interface-number</i>]	By default, no IPv6-based portal-free rule exists.

To configure a source-based portal-free rule:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Configure a source-based portal-free rule.	portal free-rule <i>rule-number</i> source { interface <i>interface-type interface-number</i> mac <i>mac-address</i> vlan <i>vlan-id</i> } *	By default, no source-based portal-free rule exists. If you specify both a VLAN and an interface, the interface must belong to the VLAN. Otherwise, the portal-free rule does not take effect.

To configure a destination-based portal-free rule:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a destination-based portal-free rule.	portal free-rule <i>rule-number</i> destination <i>host-name</i>	By default, no destination-based portal-free rule exists.

Configuring an authentication source subnet

By configuring authentication source subnets, you specify that only HTTP packets from users on the authentication source subnets can trigger portal authentication. If an unauthenticated user is not on any authentication source subnet, the access device discards all the user's HTTP packets that do not match any portal-free rule.

When you configure a portal authentication source subnet, follow these restrictions and guidelines:

- Authentication source subnets apply only to cross-subnet portal authentication.
- In direct or re-DHCP portal authentication mode, a portal user and its access interface (portal-enabled) are on the same subnet. It is not necessary to specify the subnet as the authentication source subnet. If the specified authentication source subnet is different from the access subnet of the users, the users will fail the portal authentication.
 - In direct mode, the access device regards the authentication source subnet as any source IP address.
 - In re-DHCP mode, the access device regards the authentication source subnet on an interface as the subnet to which the private IP address of the interface belongs.
- If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.
- You can configure multiple authentication source subnets. If the source subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication source subnet:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type interface-number</i>	N/A
3. Configure an IPv4 portal authentication source subnet.	portal layer3 source <i>ipv4-network-address</i> { <i>mask-length</i> <i>mask</i> }	By default, no IPv4 portal authentication source subnet is configured, and users from any subnets must pass portal authentication.

To configure an IPv6 portal authentication source subnet:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 portal authentication source subnet.	portal ipv6 layer3 source <i>ipv6-network-address</i> <i>prefix-length</i>	By default, no IPv6 portal authentication source subnet is configured, and IPv6 users from any subnets must pass portal authentication.

Configuring an authentication destination subnet

By configuring authentication destination subnets, you specify that users trigger portal authentication only when they accessing the specified subnets (excluding the destination IP addresses and subnets specified in portal-free rules). Users can access other subnets without portal authentication.

If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.

You can configure multiple authentication destination subnets. If the destination subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication destination subnet:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv4 portal authentication destination subnet.	portal free-all except destination <i>ipv4-network-address</i> { <i>mask-length</i> <i>mask</i> }	By default, no IPv4 portal authentication destination subnet is configured, and users accessing any subnets must pass portal authentication.

To configure an IPv6 portal authentication destination subnet:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 portal authentication destination subnet.	portal ipv6 free-all except destination <i>ipv6-network-address</i> <i>prefix-length</i>	By default, no IPv6 portal authentication destination subnet is configured, and users accessing any subnets must pass portal authentication.

Setting the maximum number of portal users

Perform this task to control the total number of portal users in the system, and the maximum number of IPv4 or IPv6 portal users on an interface.

If you set the maximum total number smaller than the number of current online portal users on the device, this configuration still takes effect. The online users are not affected but the system forbids new portal users to log in.

If you set the maximum number of portal users on an interface smaller than the number of current online portal users on the interface, this configuration still takes effect. The online users are not affected but the system forbids new portal users to log in from the interface.

Make sure the maximum combined number of IPv4 and IPv6 portal users specified on all interfaces does not exceed the maximum number of total portal users allowed in the system. Otherwise, the exceeding number of portal users will not be able to log in to the device.

To set the maximum number of total portal users allowed in the system:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the maximum number of total portal users.	portal max-user <i>max-number</i>	By default, no limit is set on the number of portal users in the system.

To set the maximum number of portal users on an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the maximum number of portal users on the interface.	portal { ipv4-max-user ipv6-max-user } max-number	By default, no limit is set on the number of portal users on an interface.

Specifying a portal authentication domain

An authentication domain defines a set of authentication, authorization, and accounting policies. Each portal user belongs to an authentication domain and is authenticated, authorized, and accounted in the domain.

After you specify a portal authentication domain on an interface, the device uses the specified authentication domain for AAA of all portal users on the interface, ignoring the domain names carried in the usernames. This allows for flexible portal access control.

The device selects the authentication domain for a portal user on an interface in this order:

1. ISP domain specified for the interface.
2. ISP domain carried in the username.
3. System default ISP domain. For information about the default ISP domain, see "[Configuring AAA](#)."

You can specify an IPv4 portal authentication domain, an IPv6 portal authentication domain, or both on an interface.

To specify an IPv4 portal authentication domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
3. Specify an IPv4 portal authentication domain.	portal domain <i>domain-name</i>	By default, no ISP domain is specified for IPv4 portal users on the interface.

To specify an IPv6 portal authentication domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify an IPv6 portal authentication domain.	portal ipv6 domain <i>domain-name</i>	By default, no ISP domain is specified for IPv6 portal users on the interface.

Specifying a preauthentication domain

The preauthentication domain takes effect only on portal users with IP addresses obtained through DHCP or DHCPv6.

After you configure a preauthentication domain on a portal-enabled interface, the device authorizes users on the interface as follows:

- After an unauthenticated user obtains an IP address, the user is assigned with authorization attributes configured for the preauthentication domain.
The authorization attributes in a preauthentication domain include ACL, session group profile, and CAR.
An unauthenticated user who is authorized with the authorization attributes in a preauthentication domain is called a preauthentication user.
- After the user passes portal authentication, the user is assigned with new authorization attributes from the AAA server.
- After the user goes offline, the user is reassigned with the authorization attributes in the preauthentication domain.

The preauthentication domain does not take effect on interfaces enabled with cross-subnet portal authentication.

Make sure you specify an existing ISP domain as a preauthentication domain. If the specified ISP domain does not exist, the device might operate incorrectly.

You must delete a preauthentication domain (by using the **undo portal [ipv6] pre-auth domain** command) and reconfigure it in the following situations:

- You create the ISP domain after specifying it as the preauthentication domain.
- You delete the specified ISP domain and then re-create it.

To specify a preauthentication domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify a preauthentication domain.	portal [ipv6] pre-auth domain <i>domain-name</i>	By default, no preauthentication domain is specified on an interface.

Configuring a preauthentication IP address pool for portal users

Perform this task to specify a preauthentication IP address pool for portal users. You must specify a preauthentication IP address pool on a portal-enabled interface in the following situation:

- Portal users access the network through a subinterface of the portal-enabled interface.
- The subinterface does not have an IP address.
- Portal users need to obtain IP addresses through DHCP.

After a user connects to a portal-enabled interface, the user uses an IP address for portal authentication according to the following rules:

- If the interface is configured with a preauthentication IP address pool, the user uses the following IP address:
 - If the client is configured to obtain an IP address automatically through DHCP, the user obtains an address from the specified IP address pool.
 - If the client is configured with a static IP address, the user uses the static IP address.
- If the interface has an IP address but no preauthentication IP pool configured, the user uses the static IP address or the IP address obtained from a DHCP server.
- If the interface has no IP address or preauthentication IP pool configured, the user cannot perform portal authentication.

After the user passes portal authentication, the AAA server authorizes an IP address pool for re-assigning an IP address to the user. If no authorized IP address pool is deployed, the user continues using the previous IP address.

If the portal user does not perform authentication or fails to pass authentication, the assigned IP address is still retained.

When you configure a preauthentication IP address pool, follow these guidelines and restrictions:

- This configuration takes effect only when the direct IPv4 portal authentication is enabled on the interface.
- Make sure the specified IP address pool exists and is complete. Otherwise, the user cannot obtain the IP address and cannot perform portal authentication.

To configure an IP address pool before portal authentication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a preauthentication IP address pool for portal users.	portal [ipv6] pre-auth ip-pool <i>pool-name</i>	By default, no preauthentication IP address pool is configured on an interface.

Enabling strict-checking on portal authorization information

The strict checking mode allows a portal user to stay online only when the authorized information for the user is successfully deployed on the interface.

If you enable strict ACL checking, the user will be logged out if the checking fails.

An ACL checking fails when the authorized ACL does not exist on the device or the ACL fails to be deployed.

To enable strict-checking on portal authorization information:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable strict checking mode on portal authorization information.	portal authorization acl strict-checking	By default, the strict checking mode is disabled. In this case, the portal users stay online even when the authorized ACLs do not exist or fail to be deployed.

Enabling outgoing packets filtering on a portal-enabled interface

When you enable this feature on a portal-enabled interface, the device permits the interface to send the following packets:

- Packets whose destination IP addresses are IP addresses of authenticated portal users.
- Packets that match portal-free rules.

Other outgoing packets on the interface are dropped.

To enable outgoing packets filtering on a portal-enabled interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable outgoing packets filtering.	portal [ipv6] outbound-filter enable	By default, outgoing packets filtering is disabled. The interface can send any packets.

Configuring portal detection features

Configuring online detection of portal users

Configure online detection to quickly detect abnormal logouts of portal users.

- Configure ARP or ICMP detection for IPv4 portal users.
- Configure ND or ICMPv6 detection for IPv6 portal users.

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMP or ICMPv6 detection**—Sends ICMP or ICMPv6 requests to the user at configurable intervals to detect the user status.
 - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
 - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.

- **ARP or ND detection**—Sends ARP or ND requests to the user and detects the ARP or ND entry status of the user at configurable intervals.
 - If the ARP or ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP or ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
 - If the ARP or ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

ARP and ND detections apply only to direct and re-DHCP portal authentication. ICMP detection applies to all portal authentication modes.

To configure online detection of IPv4 portal users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure online detection of IPv4 portal users.	portal user-detect type { arp icmp } [retry <i>retries</i>] [interval <i>interval</i>] [idle <i>time</i>]	By default, this feature is disabled on the interface.

To configure online detection of IPv6 portal users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure online detection of IPv6 portal users.	portal ipv6 user-detect type { icmpv6 nd } [retry <i>retries</i>] [interval <i>interval</i>] [idle <i>time</i>]	By default, this feature is disabled on the interface.

Configuring portal authentication server detection

During portal authentication, if the communication between the access device and portal authentication server is broken, both of the following occur:

- New portal users are not able to log in.
- The online portal users are not able to log out normally.

To address this problem, the access device needs to be able to detect the reachability changes of the portal server quickly and take corresponding actions to deal with the changes.

With the portal authentication server detection feature, the device periodically detects portal packets sent by a portal authentication server to determine the reachability of the server. If the device receives a portal packet within a detection timeout (**timeout** *timeout*) and the portal packet is valid, the device considers the portal authentication server to be reachable. Otherwise, the device considers the portal authentication server to be unreachable.

Portal packets include user login packets, user logout packets, and heartbeat packets. Heartbeat packets are periodically sent by a server. By detecting heartbeat packets, the device can detect the server's actual status more quickly than by detecting other portal packets.

Only the IMC portal authentication server supports sending heartbeat packets. To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the IMC portal authentication server.

You can configure the device to take one or more of the following actions when the server reachability status changes:

- Sending a trap message to the NMS. The trap message contains the name and current state of the portal authentication server.
- Sending a log message, which contains the name, the current state, and the original state of the portal authentication server.
- Enabling portal fail-permit. When the portal authentication server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see ["Configuring the portal fail-permit feature."](#)

To configure portal authentication server detection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A-
2. Enter portal authentication server view.	portal server <i>server-name</i>	N/A
3. Configure portal authentication server detection.	server-detect [timeout <i>timeout</i>] { log trap } *	By default, portal authentication server detection is disabled. This feature takes effect regardless of whether portal authentication is enabled on an interface or not.

Configuring portal Web server detection

A portal authentication process cannot complete if the communication between the access device and the portal Web server is broken. To address this problem, you can enable portal Web server detection on the access device.

With the portal Web server detection feature, the access device simulates a Web access process to initiate a TCP connection to the portal Web server. If the TCP connection can be established successfully, the access device considers the detection successful, and the portal Web server is reachable. Otherwise, it considers the detection to have failed. Portal authentication status on interfaces of the access device does not affect the portal Web server detection feature.

You can configure the following detection parameters:

- **Detection interval**—Interval at which the device detects the server reachability.
- **Maximum number of consecutive failures**—If the number of consecutive detection failures reaches this value, the access device considers that the portal Web server is unreachable.

You can configure the device to take one or more of the following actions when the server reachability status changes:

- Sending a trap message to the NMS. The trap message contains the name and current state of the portal Web server.
- Sending a log message, which contains the name, the current state, and the original state of the portal Web server.
- Enabling portal fail-permit. When the portal Web server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see ["Configuring the portal fail-permit feature."](#)

To configure portal Web server detection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter portal Web server view.	portal web-server <i>server-name</i>	N/A
3. Configure portal Web server detection.	server-detect [<i>interval interval</i>] [retry <i>retries</i>] { log trap } *	By default, portal Web server detection is disabled. This feature takes effect regardless of whether portal authentication is enabled on an interface or not.

Configuring portal user synchronization

Once the access device loses communication with a portal authentication server, the portal user information on the access device and that on the portal authentication server might be inconsistent after the communication resumes. To address this problem, the device provides the portal user synchronization feature. This feature is implemented by sending and detecting portal synchronization packets, as follows:

1. The portal authentication server sends the online user information to the access device in a synchronization packet at the user heartbeat interval, which is set on the portal authentication server.
2. Upon receiving the synchronization packet, the access device compares the users carried in the packet with its own user list. If a user contained in the packet does not exist on the access device, the access device informs the portal authentication server to delete the user. The access device starts the synchronization detection timer (**timeout** *timeout*) immediately when a user logs in. If the user does not appear in any synchronization packet within a synchronization detection interval, the access device considers the user does not exist on the portal authentication server and logs the user out.

Portal user synchronization requires a portal authentication server to support the portal user heartbeat function. Only the IMC portal authentication server supports the portal user heartbeat function. To implement the portal user synchronization feature, you also need to configure the user heartbeat function on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the access device also deletes the user synchronization configuration for the portal authentication server.

To configure portal user information synchronization:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter portal authentication server view.	portal server <i>server-name</i>	N/A
3. Configure portal user synchronization.	user-sync <i>timeout timeout</i>	By default, portal user synchronization is disabled.

Configuring the portal fail-permit feature

Perform this task to configure the portal fail-permit feature on an interface. When the access device detects that the portal authentication server or portal Web server is unreachable, it allows users on the interface to have network access without portal authentication.

If you enable fail-permit for both a portal authentication server and a portal Web server on an interface, the interface does the following:

- Disables portal authentication when either server is unreachable.
- Resumes portal authentication when both servers are reachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

To configure portal fail-permit:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable portal fail-permit for a portal authentication server.	portal [ipv6] fail-permit server <i>server-name</i>	By default, portal fail-permit is disabled for a portal authentication server.
4. Enable portal fail-permit for a portal Web server.	portal [ipv6] apply web-server <i>server-name</i> fail-permit	By default, portal fail-permit is disabled for a portal Web server.

Configuring BAS-IP for portal packets sent to the portal authentication server

If the device runs Portal 2.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

If IPv4 portal authentication is enabled on an interface, you can configure the BAS-IP attribute on the interface. If IPv6 portal authentication is enabled on an interface, you can configure the BAS-IPv6 attribute on the interface.

After this attribute is configured, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS-IP or BAS-IPv6 address. If the attribute is not configured, the source IP address of the portal packets is the IP address of the packet output interface.

During a re-DHCP portal authentication or mandatory user logout process, the device sends portal notification packets to the portal authentication server. For the authentication or logout process to complete, make sure the BAS-IP/BAS-IPv6 attribute is the same as the device IP or IPv6 address specified on the portal authentication server.

To configure the BAS-IP attribute for portal packets sent to the portal authentication server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure BAS-IP for IPv4 portal packets sent to the portal authentication server.	portal bas-ip <i>ipv4-address</i>	By default: - The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. - The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's output interface.
4. Configure BAS-IPv6 for IPv6 portal packets sent to the portal authentication server.	portal bas-ipv6 <i>ipv6-address</i>	By default: - The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet. - The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's output interface.

Enabling portal roaming

Portal roaming takes effect only on portal users logging in from VLAN interfaces. It does not take effect on portal users logging in from common Layer 3 interface.

If portal roaming is enabled on a VLAN interface, an online portal user can access resources from any Layer 2 port in the VLAN without re-authentication.

If portal roaming is disabled, to access external network resources from a Layer 2 port different from the current access port in the VLAN, the user must do the following:

- First log out from the current port.
- Then re-authenticate on the new Layer 2 port.

To enable portal roaming:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable portal roaming.	portal roaming enable	By default, portal roaming is disabled. You cannot enable portal roaming when login users exist on the device.

Specifying a format for the NAS-Port-ID attribute

RADIUS servers from different vendors might require different formats of the NAS-Port-ID attribute in the RADIUS packets. You can specify the NAS-Port-ID attribute format as required.

The device supports the NAS-Port-ID attribute in format 1, format 2, format 3, and format 4. For more information about the formats, see *Security Command Reference*.

To specify a format for the NAS-Port-ID attribute:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the format for the NAS-Port-ID attribute.	portal nas-port-id format { 1 2 3 4 }	By default, the format for the NAS-Port-ID attribute is format 2.

Logging out portal users

Logging out a user terminates the authentication process for the user or removes the user from the authenticated users list.

To log out users:

Step	Command
1. Enter system view.	system-view
2. Log out IPv4 portal users.	portal delete-user { ipv4-address all interface interface-type interface-number }
3. Log out IPv6 portal users.	portal delete-user { all interface interface-type interface-number ipv6 ipv6-address }

Configuring Web redirect

Web redirect is a simplified portal feature. With Web redirect, a user does not perform portal authentication but is directly redirected to the specified URL on the first Web access attempt in a browser. After the specified redirect interval, the user is redirected from the visiting website to the specified URL again.

Web redirect can provide ISPs with extended services. For example, the ISPs can place advertisements and publish information on the redirected webpage.

On interfaces where Web redirect is enabled, you can configure the Web redirect track feature to track the link state and signal information for an interface. This feature pushes a destination-unreachable notification webpage to users who attempt to access the Internet when it detects the following situations:

- The tracked interface is down.
- The tracked interface receives 2G signal or no signal.

In the current software version, this feature can track signal information only for Etherchannel interfaces.

On Etherchannel interfaces, both Web redirect and portal authentication can be enabled at the same time. When portal authentication, Web redirect, and Web redirect track are all enabled on an interface, the device redirects users on the interface as follows:

- The device redirects the first HTTP request of a user to the specified URL. Then, the device redirects the next HTTP request of the user to the portal authentication page. After the user logs off, the user is redirected to the specified URL again at the first Web access.
- After the specified redirect interval, a user is redirected to the specified URL regardless of whether the user is online or not. This process does not cause online users to log off.

When you configure Web redirect, follow these restrictions and guidelines:

- On Etherchannel interfaces, both Web redirect and portal authentication can be enabled at the same time. On other types of interfaces, Web redirect does not work when both Web redirect and portal authentication are enabled.

- The Web redirect track feature applies to IPv4 users only.
- The Web redirect track feature requires that the webpage to which the redirect URL points must be configured on the device. The redirect URL is specified by the **web-redirect url** command.

To configure Web redirect:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure Web redirect.	web-redirect [ipv6] url <i>url-string</i> [interval <i>interval</i>]	By default, Web redirect is disabled.
4. (Optional.) Configure Web redirect track.	web-redirect track interface <i>interface-type interface-number</i>	By default, Web redirect track is disabled.

Applying a NAS-ID profile to an interface

By default, the device sends its device name in the NAS-Identifier attribute of all RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to a portal-enabled interface. If no NAS-ID profile is specified on the interface or no matching NAS-ID is found in the specified profile, the device uses the device name as the interface NAS-ID.

To apply a NAS-ID profile to an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a NAS-ID profile and enter NAS-ID profile view.	aaa nas-id profile <i>profile-name</i>	For more information about this command, see <i>Security Command Reference</i> .
3. Configure a NAS ID and VLAN binding in the profile.	nas-id <i>nas-identifier</i> bind vlan <i>vlan-id</i>	For more information about this command, see <i>Security Command Reference</i> .
4. Return to system view.	quit	N/A
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Specify the NAS-ID profile on the interface.	portal nas-id-profile <i>profile-name</i>	By default, no NAS-ID profile is specified on the interface.

Displaying and maintaining portal

Execute **display** commands in any view and the **reset** command in user view.

Task	Command
Display portal rules on an interface (centralized devices in standalone mode).	display portal rule { all dynamic static } interface <i>interface-type interface-number</i>
Display portal rules on an interface (distributed devices in standalone mode).	display portal rule { all dynamic static } interface <i>interface-type interface-number</i> [slot slot-id]
Display portal rules on an interface (distributed devices in IRF mode).	display portal rule { all dynamic static } interface <i>interface-type interface-number</i> [chassis chassis-number slot slot-number]
Display portal configuration and portal running state information on an interface.	display portal interface <i>interface-type interface-number</i>
Display portal authentication server information.	display portal server [<i>server-name</i>]
Display portal Web server information.	display portal web-server [<i>server-name</i>]
Display packet statistics for portal authentication servers.	display portal packet statistics [server server-name]
Display portal user information.	display portal user { all interface <i>interface-type interface-number</i> ip <i>ip-address</i> ipv6 <i>ipv6-address</i> pre-auth [interface <i>interface-type interface-number</i> ip <i>ip-address</i> ipv6 <i>ipv6-address</i>] } [verbose]
Clear packet statistics for portal authentication servers.	reset portal packet statistics [server server-name]
Display Web redirect rule information (centralized devices in standalone mode).	display web-redirect rule interface <i>interface-type interface-number</i>
Display Web redirect rule information (distributed devices in standalone mode/centralized devices in IRF mode).	display web-redirect rule interface <i>interface-type interface-number</i> [slot slot-number]
Display Web redirect rule information (distributed devices in IRF mode).	display web-redirect rule interface <i>interface-type interface-number</i> [chassis chassis-number slot slot-number]

Portal configuration examples

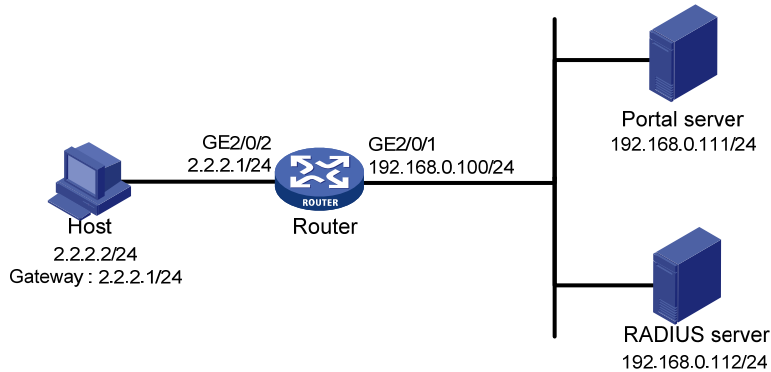
Configuring direct portal authentication

Network requirements

As shown in [Figure 51](#), the host is directly connected to the router (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication, so the host can access only the portal server before passing the authentication and access other network resources after passing the authentication.

Figure 51 Network diagram



Configuration prerequisites

- Configure IP addresses for the host, router, and servers as shown in [Figure 51](#) and make sure they can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.

Configuring the portal authentication server on IMC PLAT 5.0

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:
 - a. Log in to IMC and click the **Service** tab.
 - b. Select **User Access Manager > Portal Service Management > Server** from the navigation tree to enter the portal server configuration page, as shown in [Figure 52](#).
 - c. Configure the portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 52 Portal server configuration

Service>>User Access Manager>>Portal Service Management >> Server

Portal Server Configuration

Basic Information

* Log Level	Info	* Request Timeout	5	Seconds
* Server Heartbeat Interval	20	* User Heartbeat Interval	5	Minutes

Portal Page:

Advanced Information

Service Type List

Total Items: 0.

Service Type ID	Service Type	Delete

2. Configure the IP address group:
 - a. Select **User Access Manager > Portal Service Management > IP Group** from the navigation tree to enter the portal IP address group configuration page.
 - b. Click **Add** to enter the page shown in [Figure 53](#).
 - c. Enter the IP group name.
 - d. Enter the start IP address and end IP address of the IP group.
Make sure the host IP address is in the IP group.
 - e. Select a service group.
This example uses the default group **Ungrouped**.
 - f. Select **Normal** from the **Action** list.
 - g. Click **OK**.

Figure 53 Adding an IP address group

The screenshot shows the 'Add IP Group' configuration page. The breadcrumb navigation at the top is: Service >> User Access Manager >> Portal Service Management >> Portal IP Group Configuration >> Add IP Group. The form has a title bar 'Add IP Group' and contains the following fields:

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
Service Group	Ungrouped
* Action	Normal

At the bottom right of the form are two buttons: 'OK' and 'Cancel'.

3. Add a portal device:
 - a. Select **User Access Manager > Portal Service Management > Device** from the navigation tree to enter the portal device configuration page.
 - b. Click **Add** to enter the page shown in [Figure 54](#).
 - c. Enter the device name **NAS**.
 - d. Enter the IP address of the router's interface connected to the host.
 - e. Enter the key, which must be the same as that configured on the router.
 - f. Set whether to enable IP address reallocation.
This example uses direct portal authentication, and therefore select **No** from the **Reallocate IP** list.
 - g. Select whether to support sever heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - h. Click **OK**.

Figure 54 Adding a portal device

Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Add Device

Add Device

* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No	* Support User Heartbeat	No
* Support Server Heartbeat	No		
* Service Group	Ungrouped		
Device Description			

OK Cancel

4. Associate the portal device with the IP address group:
 - a. As shown in Figure 55, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.
 - b. Click **Add** to enter the page shown in Figure 56.
 - c. Enter the port group name.
 - d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 55 Device list

Device Information List							
Add							
1-2 of 2, Page 1 of 1.				Items per Page: 8 15 [50] 100 200			
Device Name	Version	Service Group	IP Address	Port Group Information Management	Details	Modify	Delete
NAS	Portal 2.0	Ungrouped	2.2.2.1				

Figure 56 Adding a port group

Service >> User Access Manager >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add

Add Port Group Info

* Port Group Name	group	* Language	Dynamic Detection
* Start Port	0	* End Port	zzzzz
* Protocol	HTTP	* Quick Authentication	No
* NAT or Not	No	* Error Transparent Transmission	Yes
* Authentication Type	CHAP	* IP Group	Portal_user
* Heartbeat Interval	10	* Heartbeat Timeout	30
	Minutes		Minutes
User Domain		Port Group Description	
User Attribute Type		Default Authentication Page	index_default.jsp
Default Authentication Type	Web Identity AuthN		

OK Cancel

5. Select **User Access Manager > Service Parameters > Validate System Configuration** from the navigation tree to validate the configurations.

Configuring the portal server on IMC PLAT 7.1

In this example, the portal server runs on IMC PLAT 7.1 (E0303) and IMC EIA 7.1 (F0303).

1. Configure the portal authentication server:
 - a. Log in to IMC and click the **User** tab.
 - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to enter the portal server configuration page, as shown in [Figure 57](#).
 - c. Configure the portal server parameters as needed.
This example uses the default values.
 - d. Click **OK**.

Figure 57 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4 Server Heartbeat Interval(Seconds) * 20

User Heartbeat Interval(Minutes) * 5 LB Device Address

Portal Web

Request Timeout(Seconds) * 15 Packet Code

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.0.111:8080/portal/

Advanced Information

Service Type List

Add

Total Items: 0.

2. Configure the IP address group:
 - a. Select **User Access Policy > Portal Service > IP Group** from the navigation tree to enter the portal IP address group configuration page.
 - b. Click **Add** to enter the page shown in [Figure 58](#).
 - c. Enter the IP group name.
 - d. Enter the start IP address and end IP address of the IP group.
Make sure the client IP address (2.2.2.2) is in the IP group.
 - e. Select a service group.
This example uses the default group **Ungrouped**.
 - f. Select **Normal** from the **Action** list.
 - g. Click **OK**.

Figure 58 Adding an IP address group

User > User Access Policy > Portal Service > IP Group > Add IP Group

Help

Add IP Group

IP Group Name * Portal_user

Start IP * 2.2.2.1

End IP * 2.2.2.255

Service Group Ungrouped

Action * Normal

OK Cancel

3. Add a portal device:
 - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to enter the portal device configuration page.
 - b. Click **Add** to enter the page shown in [Figure 59](#).
 - c. Enter the device name.
 - d. Enter the IP address of the router's interface that exchanges information with the portal server.
 - e. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - f. Enter the key, which must be the same as that configured on the router.
 - g. Select **Directly Connected** from the **Access Method** list.
 - h. Click **OK**.

Figure 59 Adding a portal device

User > User Access Policy > Portal Service > Device > Add Device

Help

Add Device

Device Information

Device Name * NAS

Version * Portal 2.0

Listening Port * 2000

Authentication Retries * 0

Support Server Heartbeat * No

Key * *****

Access Method * Directly Connected

Device Description

Service Group * Ungrouped

IP Address * 2.2.2.1

Local Challenge * No

Logout Retries * 1

Support User Heartbeat * No

Confirm Key * *****

OK Cancel

4. Associate the portal device with the IP address group:
 - a. As shown in Figure 60, click the **Port Group Information Management** icon for device **NAS** to enter the port group configuration page.
 - b. Click **Add** to enter the page shown in Figure 61.
 - c. Enter the port group name.
 - d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 60 Device list

Figure 61 Adding a port group

Configuring the router

1. Configure a RADIUS scheme:

Create a RADIUS scheme named rs1 and enter its view.

```
<Router> system-view
[Router] radius scheme rs1
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Router-radius-rs1] primary authentication 192.168.0.112
```

```
[Router-radius-rs1] primary accounting 192.168.0.112
```

```
[Router-radius-rs1] key authentication simple radius
```

```
[Router-radius-rs1] key accounting simple radius
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Router-radius-rs1] user-name-format without-domain
```

```
[Router-radius-rs1] quit
```

Enable RADIUS session control.

```
[Router] radius session-control enable
```

2. Configure an authentication domain:

Create an ISP domain named **dm1** and enter its view.

```
[Router] domain dm1
```

Configure AAA methods for the ISP domain.

```
[Router-isp-dm1] authentication portal radius-scheme rs1
```

```
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
```

```
[Router-isp-dm1] quit
```

Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Router] domain default enable dm1
```

3. Configure portal authentication:

Configure a portal authentication server.

```
[Router] portal server newpt
```

```
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[Router-portal-server-newpt] port 50100
```

```
[Router-portal-server-newpt] quit
```

Configure a portal Web server.

```
[Router] portal web-server newpt
```

```
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[Router-portal-websvr-newpt] quit
```

Enable direct portal authentication on GigabitEthernet 2/0/2.

```
[Router] interface gigabitethernet 2/0/2
```

```
[Router-GigabitEthernet2/0/2] portal enable method direct
```

Reference the portal Web server newpt on GigabitEthernet 2/0/2.

```
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
```

Configure the BAS-IP as 2.2.2.1 for portal packets sent from GigabitEthernet 2/0/2 to the portal authentication server.

```
[Router-GigabitEthernet2/0/2] portal bas-ip 2.2.2.1
```

```
[Router-GigabitEthernet2/0/2] quit
```

Verifying the configuration

Verify that the portal configuration has taken effect.

```
[Router] display portal interface gigabitethernet 2/0/2
```

```
Portal information of GigabitEthernet 2/0/2
```

```
NAS-ID profile: Not configured
```

```

    Authorization : Strict checking
    ACL           : Disabled
IPv4:
    Portal status: Enabled
    Authentication type: Direct
    Portal Web server: newpt
    Authentication domain: Not configured
    Pre-auth IP pool: Not configured
    BAS-IP: 2.2.2.1
    User Detection: Not configured
    Action for server detection:
        Server type    Server name                Action
        --            --
    Layer3 source network:
        IP address          Mask

    Destination authenticate subnet:
        IP address          Mask

IPv6:
    Portal status: Disabled
    Authentication type: Disabled
    Portal Web server: Not configured
    Authentication domain: Not configured
    Pre-auth IP pool: Not configured
    BAS-IPv6: Not configured
    User detection: Not configured
    Action for server detection:
        Server type    Server name                Action
        --            --
    Layer3 source network:
        IP address          Prefix length

    Destination authenticate subnet:
        IP address          Prefix length

```

A user can perform portal authentication by using the HPE iNode client or through Web page. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

After the user passes authentication, use the following command to display information about the portal user.

```
[Router] display portal user interface gigabitethernet 2/0/2
```

```
Total portal users: 1
```

```
Username: abc
```

```
Portal server: newpt
```

```
State: Online
```

```
VPN instance: N/A
```

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	2.2.2.2	--	GigabitEthernet2/0/2

```
Authorization information:
```

DHCP IP pool: N/A
Session group profile: N/A
ACL: N/A
CAR: N/A

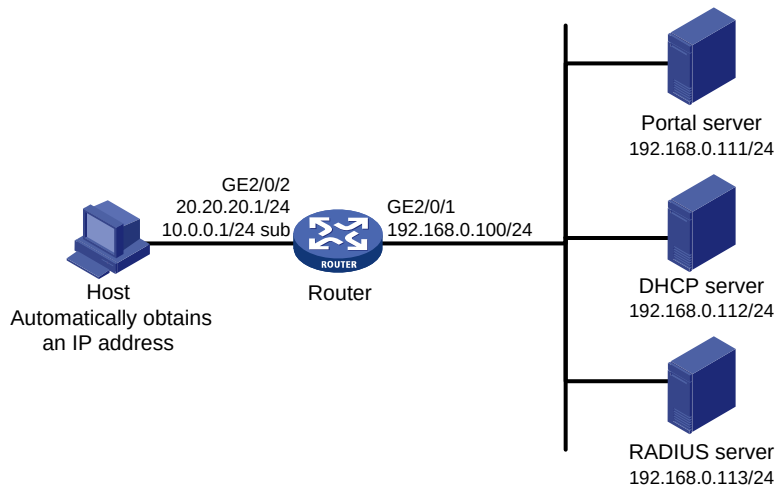
Configuring re-DHCP portal authentication

Network requirements

As shown in [Figure 62](#), the host is directly connected to the router (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure re-DHCP portal authentication. Before passing the authentication, the host is assigned a private IP address. After passing the authentication, the host gets a public IP address and can access Internet resources.

Figure 62 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in [Figure 62](#) and make sure the host, router, and servers can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
 - The router must be configured as a DHCP relay agent.
 - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).

For information about DHCP relay agent configuration, see *Layer 3—IP Services Configuration Guide*.

- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the router's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.

Configuration procedure

Perform the following tasks on the router.

1. Configure a RADIUS scheme:

Create a RADIUS scheme named rs1 and enter its view.

```
<Router> system-view
```

```
[Router] radius scheme rs1
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Router-radius-rs1] primary authentication 192.168.0.113
```

```
[Router-radius-rs1] primary accounting 192.168.0.113
```

```
[Router-radius-rs1] key authentication simple radius
```

```
[Router-radius-rs1] key accounting simple radius
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Router-radius-rs1] user-name-format without-domain
```

```
[Router-radius-rs1] quit
```

Enable RADIUS session control.

```
[Router] radius session-control enable
```

2. Configure an authentication domain:

Create an ISP domain named **dm1** and enter its view.

```
[Router] domain dm1
```

Configure AAA methods for the ISP domain.

```
[Router-isp-dm1] authentication portal radius-scheme rs1
```

```
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
```

```
[Router-isp-dm1] quit
```

Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Router] domain default enable dm1
```

3. Configure DHCP relay and authorized ARP:

Configure DHCP relay.

```
[Router] dhcp enable
```

```
[Router] dhcp relay client-information record
```

```
[Router] interface gigabitethernet 2/0/2
```

```
[Router-GigabitEthernet2/0/2] ip address 20.20.20.1 255.255.255.0
```

```
[Router-GigabitEthernet2/0/2] ip address 10.0.0.1 255.255.255.0 sub
```

```
[Router-GigabitEthernet2/0/2] dhcp select relay
```

```
[Router-GigabitEthernet2/0/2] dhcp relay server-address 192.168.0.112
```

Enable authorized ARP.

```
[Router-GigabitEthernet2/0/2] arp authorized enable
```

```
[Router-GigabitEthernet2/0/2] quit
```

4. Configure portal authentication:

Configure a portal authentication server.

```
[Router] portal server newpt
```

```
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[Router-portal-server-newpt] port 50100
```

```
[Router-portal-server-newpt] quit
```

```
# Configure a portal Web server.
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
# Enable re-DHCP portal authentication on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal enable method redhcp
# Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
# Configure the BAS-IP as 20.20.20.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 20.20.20.1
[Router-GigabitEthernet2/0/2] quit
```

Verifying the configuration

```
# Verify that the portal configuration has taken effect.
[Router] display portal interface gigabitethernet 2/0/2
Portal information of GigabitEthernet2/0/2
  NAS-ID profile: Not configured
  Authorization : Strict checking
  ACL           : Disabled
IPv4:
  Portal status: Enabled
  Authentication type: Redhcp
  Portal Web server: newpt
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IP: 20.20.20.1
  User Detection: Not configured
  Action for server detection:
    Server type  Server name  Action
    --          --          --
  Layer3 source network:
    IP address  Mask
    --          --
  Destination authenticate subnet:
    IP address  Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IPv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type  Server name  Action
    --          --          --
  Layer3 source network:
```


IP address

Prefix length

Destination authenticate subnet:

IP address

Prefix length

A user can perform portal authentication by using the HPE iNode client or through Web page. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

After the user passes authentication, use the following command to display information about the portal user.

```
[Router] display portal user interface gigabitethernet 2/0/2
```

Total portal users: 1

Username: abc

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	20.20.20.2	--	GigabitEthernet2/0/2

Authorization information:

DHCP IP pool: N/A

Session group profile: N/A

ACL: N/A

CAR: N/A

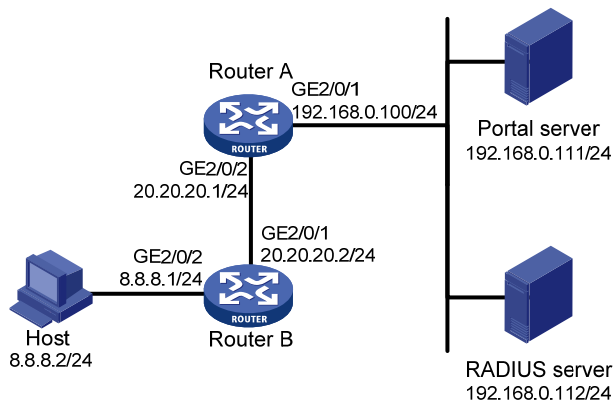
Configuring cross-subnet portal authentication

Network requirements

As shown in Figure 63, Router A supports portal authentication. The host accesses Router A through Router B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Router A for cross-subnet portal authentication. Before passing the authentication, the host can access only the portal server. After passing the authentication, the user can access Internet resources.

Figure 63 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in [Figure 63](#) and make sure the host, router, and servers can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- Make sure the IP address of the portal device added on the portal authentication server is the IP address (20.20.20.1) of the router's interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

Configuration procedure

Perform the following tasks on Router A.

1. Configure a RADIUS scheme:

Create a RADIUS scheme named rs1 and enter its view.

```
<RouterA> system-view
```

```
[RouterA] radius scheme rs1
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
```

```
[RouterA-radius-rs1] primary accounting 192.168.0.112
```

```
[RouterA-radius-rs1] key authentication simple radius
```

```
[RouterA-radius-rs1] key accounting simple radius
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[RouterA-radius-rs1] user-name-format without-domain
```

```
[RouterA-radius-rs1] quit
```

Enable RADIUS session control.

```
[Router] radius session-control enable
```

2. Configure an authentication domain:

Create an ISP domain named **dm1** and enter its view.

```
[RouterA] domain dm1
```

Configure AAA methods for the ISP domain.

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
```

```
[RouterA-isp-dm1] authorization portal radius-scheme rs1
```

```
[RouterA-isp-dm1] accounting portal radius-scheme rs1
```

```
[RouterA-isp-dm1] quit
```

Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Router] domain default enable dm1
```

3. Configure portal authentication:

Configure a portal authentication server.

```
[RouterA] portal server newpt
```

```
[RouterA-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[RouterA-portal-server-newpt] port 50100
```

```
[RouterA-portal-server-newpt] quit
```

Configure a portal Web server.

```
[Router] portal web-server newpt
```

```
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[RouterA-portal-websvr-newpt] quit
```

Enable cross-subnet portal authentication on GigabitEthernet 2/0/2.

```

[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] portal enable method layer3
# Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[RouterA-GigabitEthernet2/0/2] portal apply web-server newpt
# Configure the BAS-IP as 20.20.20.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[RouterA-GigabitEthernet2/0/2] portal bas-ip 20.20.20.1
[RouterA-GigabitEthernet2/0/2] quit

```

On Router B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

Verifying the configuration

Verify that the portal configuration has taken effect.

```

[Router] display portal interface gigabitethernet 2/0/2
Portal information of GigabitEthernet2/0/2
  NAS-ID profile: Not configured
  Authorization : Strict checking
  ACL           : Disabled
IPv4:
  Portal status: Enabled
  Authentication type: Layer3
  Portal Web server: newpt
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IP: 20.20.20.1
  User Detection: Not configured
  Action for server detection:
    Server type   Server name           Action
    --           --
  Layer3 source network:
    IP address           Mask
    Destination authenticate subnet:
    IP address           Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IPv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type   Server name           Action
    --           --
  Layer3 source network:
    IP address           Prefix length
    Destination authenticate subnet:

```

IP address

Prefix length

A user can perform portal authentication by using the HPE iNode client or through Web page. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

After the user passes authentication, use the following command to display information about the portal user.

```
[Router] display portal user interface gigabitethernet 2/0/2
```

Total portal users: 1

Username: abc

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	8.8.8.2	--	GigabitEthernet2/0/2

Authorization information:

DHCP IP pool: N/A

Session group profile: N/A

ACL: N/A

CAR: N/A

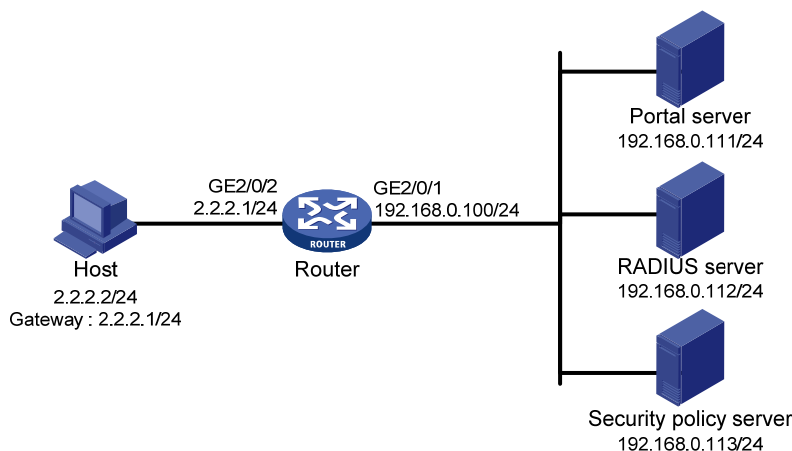
Configuring extended direct portal authentication

Network requirements

As shown in [Figure 64](#), the host is directly connected to the router (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended direct portal authentication. If the host fails security check after passing identity authentication, it can access only subnet 192.168.0.0/24. After passing security check, the host can access Internet resources.

Figure 64 Network diagram



Configuration prerequisites

- Configure IP addresses for the host, router, and servers as shown in [Figure 64](#) and make sure they can reach each other.

- Configure the RADIUS server correctly to provide authentication and accounting functions.

Configuration procedure

Perform the following tasks on the router.

1. Configure a RADIUS scheme:

Create a RADIUS scheme named **rs1** and enter its view.

```
<Router> system-view
```

```
[Router] radius scheme rs1
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Router-radius-rs1] primary authentication 192.168.0.112
```

```
[Router-radius-rs1] primary accounting 192.168.0.112
```

```
[Router-radius-rs1] key accounting simple radius
```

```
[Router-radius-rs1] key authentication simple radius
```

```
[Router-radius-rs1] user-name-format without-domain
```

Specify the security policy server.

```
[Router-radius-rs1] security-policy-server 192.168.0.113
```

```
[Router-radius-rs1] quit
```

Enable RADIUS session control.

```
[Router] radius session-control enable
```

2. Configure an authentication domain:

Create an ISP domain named **dm1** and enter its view.

```
[Router] domain dm1
```

Configure AAA methods for the ISP domain.

```
[Router-isp-dm1] authentication portal radius-scheme rs1
```

```
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
```

```
[Router-isp-dm1] quit
```

Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Router] domain default enable dm1
```

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

```
[Router] acl advanced 3000
```

```
[Router-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Router-acl-ipv4-adv-3000] rule deny ip
```

```
[Router-acl-ipv4-adv-3000] quit
```

```
[Router] acl advanced 3001
```

```
[Router-acl-ipv4-adv-3001] rule permit ip
```

```
[Router-acl-ipv4-adv-3001] quit
```

NOTE:

Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure portal authentication:

Configure a portal authentication server.

```
[Router] portal server newpt
```

```
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```

[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
# Configure a portal Web server.
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
# Enable direct portal authentication on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal enable method direct
# Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
# Configure the BAS-IP as 2.2.2.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 2.2.2.1
[Router-GigabitEthernet2/0/2] quit

```

Verifying the configuration

```

# Verify that the portal configuration has taken effect.
[Router] display portal interface gigabitethernet 2/0/2
Portal information of GigabitEthernet2/0/2
  NAS-ID profile: Not configured
  Authorization : Strict checking
  ACL           : Disabled
IPv4:
  Portal status: Enabled
  Authentication type: Direct
  Portal Web server: newpt
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IP: 2.2.2.1
  User Detection: Not configured
  Action for server detection:
    Server type   Server name           Action
    --           --
  Layer3 source network:
    IP address           Mask
    Destination authenticate subnet:
    IP address           Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Pre-auth IP pool: Not configured
  BAS-IPv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type   Server name           Action

```

```

--
Layer3 source network:
    IP address
--
    Prefix length

Destination authenticate subnet:
    IP address
--
    Prefix length

Before passing portal authentication, a user that uses the HPE iNode client can access only the
authentication page http://192.168.0.111:8080/portal. All Web requests from the user will be
redirected to the authentication page.

• The user can access the resources permitted by ACL 3000 after passing only identity
  authentication.
• The user can access Internet resources permitted by ACL 3001 after passing both identity
  authentication and security check.

# After the user passes identity authentication and security check, use the following command to
display information about the portal user.
[Router] display portal user interface gigabitethernet 2/0/2
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN   Interface
  0015-e9a6-7cfe 2.2.2.2  --    GigabitEthernet2/0/2
Authorization information:
  DHCP IP pool: N/A
  Session group profile: N/A
  ACL: 3001
  CAR: N/A

```

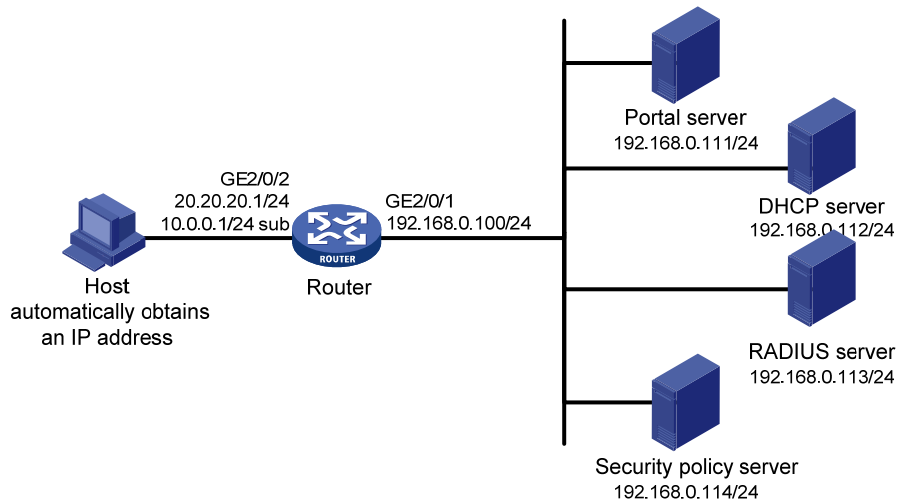
Configuring extended re-DHCP portal authentication

Network requirements

As shown in [Figure 65](#), the host is directly connected to the router (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended re-DHCP portal authentication. Before passing portal authentication, the host is assigned a private IP address. After passing portal identity authentication, the host obtains a public IP address and accepts security check. If the host fails the security check, it can access only subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.

Figure 65 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in [Figure 65](#) and make sure the host, router, and servers can reach each other.
 - Configure the RADIUS server correctly to provide authentication and accounting functions.
 - For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
 - For re-DHCP portal authentication:
 - The router must be configured as a DHCP relay agent.
 - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).
- For information about DHCP relay agent configuration, see *Layer 3—IP Services Configuration Guide*.
- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the router's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.

Configuration procedure

Perform the following tasks on the router.

1. Configure a RADIUS scheme:

Create a RADIUS scheme named **rs1** and enter its view.

```
<Router> system-view
```

```
[Router] radius scheme rs1
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Router-radius-rs1] primary authentication 192.168.0.113
```

```
[Router-radius-rs1] primary accounting 192.168.0.113
```

```
[Router-radius-rs1] key authentication simple radius
```

```
[Router-radius-rs1] key accounting simple radius
```

```
[Router-radius-rs1] user-name-format without-domain
```

Specify the security policy server.

```
[Router-radius-rs1] security-policy-server 192.168.0.114
```


- ```
Enable RADIUS session control.
[Router-radius-rs1] radius session-control enable
[Router-radius-rs1] quit
Enable RADIUS session control.
[Router] radius session-control enable
```
2. Configure an authentication domain:
- ```
# Create an ISP domain named dm1 and enter its view.
[Router] domain dm1
# Configure AAA methods for the ISP domain.
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
# Configure domain dm1 as the default ISP domain. If a user enters the username without the
ISP domain name at login, the authentication and accounting methods of the default domain
are used for the user.
[Router] domain default enable dm1
```
3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.
- ```
[Router] acl advanced 3000
[Router-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Router-acl-ipv4-adv-3000] rule deny ip
[Router-acl-ipv4-adv-3000] quit
[Router] acl advanced 3001
[Router-acl-ipv4-adv-3001] rule permit ip
[Router-acl-ipv4-adv-3001] quit
```

---

**NOTE:**

Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

---

4. Configure DHCP relay and authorized ARP:
- ```
# Configure DHCP relay.
[Router] dhcp enable
[Router] dhcp relay client-information record
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] ip address 20.20.20.1 255.255.255.0
[Router-GigabitEthernet2/0/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet2/0/2] dhcp select relay
[Router-GigabitEthernet2/0/2] dhcp relay server-address 192.168.0.112
# Enable authorized ARP.
[Router-GigabitEthernet2/0/2] arp authorized enable
[Router-GigabitEthernet2/0/2] quit
```
5. Configure portal authentication:
- ```
Configure a portal authentication server.
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

```
Configure a portal Web server.
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
Enable re-DHCP portal authentication on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal enable method redhcp
Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
Configure the BAS-IP as 20.20.20.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 20.20.20.1
[Router-GigabitEthernet2/0/2] quit
```

## Verifying the configuration

```
Verify that the portal configuration has taken effect.
[Router] display portal interface gigabitethernet 2/0/2
Portal information of GigabitEthernet2/0/2
 NAS-ID profile: Not configured
 Authorization : Strict checking
 ACL : Disabled
IPv4:
 Portal status: Enabled
 Authentication type: Redhcp
 Portal Web server: newpt
 Authentication domain: Not configured
 Pre-auth IP pool: Not configured
 BAS-IP: 20.20.20.1
 User Detection: Not configured
 Action for server detection:
 Server type Server name Action
 -- -- --
 Layer3 source network:
 IP address Mask
 -- --
 Destination authenticate subnet:
 IP address Mask
IPv6:
 Portal status: Disabled
 Authentication type: Disabled
 Portal Web server: Not configured
 Authentication domain: Not configured
 Pre-auth IP pool: Not configured
 BAS-IPv6: Not configured
 User detection: Not configured
 Action for server detection:
 Server type Server name Action
 -- -- --
 Layer3 source network:
```

IP address

Prefix length

Destination authenticate subnet:

IP address

Prefix length

Before passing portal authentication, a user that uses the HPE iNode client can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page.

- The user can access the resources permitted by ACL 3000 after passing only identity authentication.
- The user can access Internet resources permitted by ACL 3001 after passing both identity authentication and security check.

# After the user passes identity authentication and security check, use the following command to display information about the portal user.

```
[Router] display portal user interface gigabitethernet 2/0/2
```

Total portal users: 1

Username: abc

Portal server: newpt

State: Online

VPN instance: N/A

| MAC            | IP         | VLAN | Interface            |
|----------------|------------|------|----------------------|
| 0015-e9a6-7cfe | 20.20.20.2 | --   | GigabitEthernet2/0/2 |

Authorization information:

DHCP IP pool: N/A

Session group profile: N/A

ACL: 3001

CAR: N/A

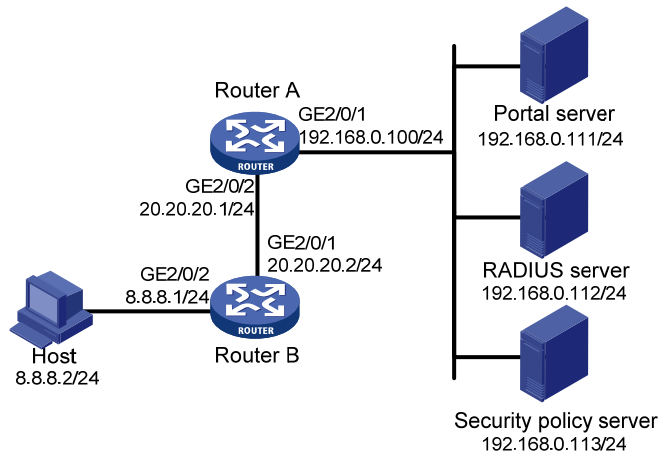
## Configuring extended cross-subnet portal authentication

### Network requirements

As shown in [Figure 66](#), Router A supports portal authentication. The host accesses Router A through Router B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Router A for extended cross-subnet portal authentication. Before passing portal authentication, the host can access only the portal server. After passing portal identity authentication, the host accepts security check. If the host fails the security check it can access only the subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.

Figure 66 Network diagram



### Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in Figure 66 and make sure the host, router, and servers can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- Make sure the IP address of the portal device added on the portal server is the IP address (20.20.20.1) of the router's interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

### Configuration procedure

Perform the following tasks on Router A.

#### 1. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1** and enter its view.

```
<RouterA> system-view
```

```
[RouterA] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
```

```
[RouterA-radius-rs1] primary accounting 192.168.0.112
```

```
[RouterA-radius-rs1] key authentication simple radius
```

```
[RouterA-radius-rs1] key accounting simple radius
```

```
[RouterA-radius-rs1] user-name-format without-domain
```

# Specify the security policy server.

```
[RouterA-radius-rs1] security-policy-server 192.168.0.113
```

```
[RouterA-radius-rs1] quit
```

# Enable RADIUS session control.

```
[RouterA] radius session-control enable
```

#### 2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[RouterA] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
```

```
[RouterA-isp-dm1] authorization portal radius-scheme rs1
```

```
[RouterA-isp-dm1] accounting portal radius-scheme rs1
```

```
[RouterA-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[RouterA] domain default enable dm1
```

**3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.**

```
[RouterA] acl advanced 3000
```

```
[RouterA-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[RouterA-acl-ipv4-adv-3000] rule deny ip
```

```
[RouterA-acl-ipv4-adv-3000] quit
```

```
[RouterA] acl advanced 3001
```

```
[RouterA-acl-ipv4-adv-3001] rule permit ip
```

```
[RouterA-acl-ipv4-adv-3001] quit
```

---

**NOTE:**

Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

---

**4. Configure portal authentication:**

# Configure a portal authentication server.

```
[RouterA] portal server newpt
```

```
[RouterA-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[RouterA-portal-server-newpt] port 50100
```

```
[RouterA-portal-server-newpt] quit
```

# Configure a portal Web server.

```
[Router] portal web-server newpt
```

```
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[RouterA-portal-websvr-newpt] quit
```

# Enable cross-subnet portal authentication on GigabitEthernet 2/0/2.

```
[RouterA] interface gigabitethernet 2/0/2
```

```
[RouterA-GigabitEthernet2/0/2] portal enable method layer3
```

# Reference the portal Web server newpt on GigabitEthernet 2/0/2.

```
[RouterA-GigabitEthernet2/0/2] portal apply web-server newpt
```

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from GigabitEthernet 2/0/2 to the portal authentication server.

```
[RouterA-GigabitEthernet2/0/2] portal bas-ip 20.20.20.1
```

```
[RouterA-GigabitEthernet2/0/2] quit
```

On Router B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

## Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Router] display portal interface gigabitethernet 2/0/2
```

```
Portal information of GigabitEthernet 2/0/2
```

```
NAS-ID profile: Not configured
```

```
Authorization : Strict checking
```

```
ACL : Disabled
```

```
IPv4:
```

```
Portal status: Enabled
```

```
Authentication type: Layer3
```

```

Portal Web server: newpt
Authentication domain: Not configured
Pre-auth IP pool: Not configured
BAS-IP: 20.20.20.1
User Detection: Not configured
Action for server detection:
 Server type Server name Action
 -- --
Layer3 source network:
 IP address Mask
Destination authenticate subnet:
 IP address Mask

```

#### IPv6:

```

Portal status: Disabled
Authentication type: Disabled
Portal Web server: Not configured
Authentication domain: Not configured
Pre-auth IP pool: Not configured
BAS-IPv6: Not configured
User detection: Not configured
Action for server detection:
 Server type Server name Action
 -- --
Layer3 source network:
 IP address Prefix length
Destination authenticate subnet:
 IP address Prefix length

```

Before passing portal authentication, a user that uses the HPE iNode client can access only the authentication page <http://192.168.0.111:8080/portal>. All Web requests from the user are redirected to the authentication page.

- The user can access the resources permitted by ACL 3000 after passing only identity authentication.
- The user can access Internet resources permitted by ACL 3001 after passing both identity authentication and security check.

# After the user passes identity authentication and security check, use the following command to display information about the portal user.

```
[Router] display portal user interface gigabitethernet 2/0/2
```

```
Total portal users: 1
```

```
Username: abc
```

```
Portal server: newpt
```

```
State: Online
```

```
VPN instance: N/A
```

| MAC            | IP      | VLAN | Interface            |
|----------------|---------|------|----------------------|
| 0015-e9a6-7cfe | 8.8.8.2 | --   | GigabitEthernet2/0/2 |

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
Session group profile: N/A
```

# Configuring portal server detection and portal user synchronization

## Network requirements

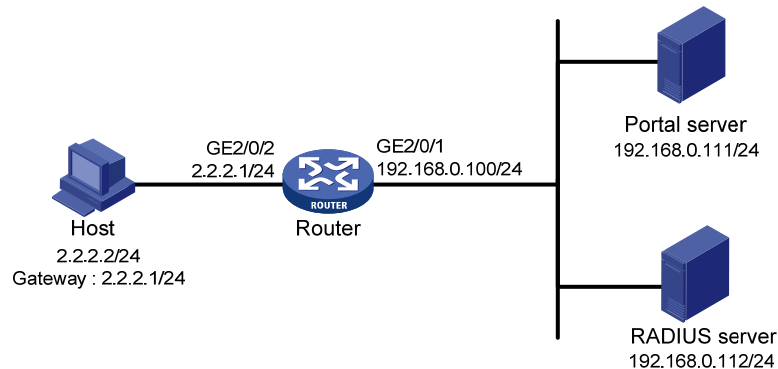
As shown in [Figure 67](#), the host is directly connected to the router (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the router, so the host can access only the portal server before passing the authentication and access Internet resources after passing the authentication.

Configure the router to do the following:

- Detect the reachability state of the portal authentication server.
- Send log messages upon state changes.
- Disable portal authentication when the authentication server is unreachable.
- Synchronize portal user information with the portal server periodically.

**Figure 67 Network diagram**



## Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in [Figure 67](#) and make sure the host, router, and servers can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- Configure the portal authentication server. Be sure to enable the server heartbeat function and the user heartbeat function.
- Configure the router (access device) as follows:
  - Configure direct portal authentication on GigabitEthernet 2/0/2, the interface to which the host is connected.
  - Configure portal authentication server detection, so that the router can detect the reachability of the portal authentication server by cooperating with the portal server heartbeat function.
  - Configure portal user synchronization, so that the router can synchronize portal user information with the portal authentication server by cooperating with the portal user heartbeat function.

## Configuring the portal authentication server on IMC PLAT 5.0

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:
  - a. Log in to IMC and click the **Service** tab.
  - b. Select **User Access Manager > Portal Service Management > Server** from the navigation tree to enter the portal server configuration page, as shown in [Figure 68](#).
  - c. Configure the portal server heartbeat interval and user heartbeat interval.
  - d. Use the default settings for other parameters.
  - e. Click **OK**.

**Figure 68 Portal authentication server configuration**

Service>>User Access Manager>>Portal Service Management >> Server

**Portal Server Configuration**

**Basic Information**

\* Log Level: Info

\* Request Timeout: 5 Seconds

\* Server Heartbeat Interval: 20 Seconds

\* User Heartbeat Interval: 5 Minutes

Portal Page: http://192.168.0.111:8080/portal

**Advanced Information**

**Service Type List**

Add

Total Items: 0.

| Service Type ID | Service Type | Delete |
|-----------------|--------------|--------|
|-----------------|--------------|--------|

OK

2. Configure the IP address group:
  - a. Select **User Access Manager > Portal Service Management > IP Group** from the navigation tree to enter the portal IP address group configuration page.
  - b. Click **Add** to enter the page shown in [Figure 69](#).
  - c. Enter the IP group name.
  - d. Enter the start IP address and end IP address of the IP group.  
Make sure the host IP address is in the IP group.
  - e. Select a service group.  
This example uses the default group **Ungrouped**.
  - f. Select **Normal** from the **Action** list.
  - g. Click **OK**.



**Figure 69 Adding an IP address group**

Service>>User Access Manager>>Portal Service Management>>Portal IP Group Configuration>>Add IP Group

---

**Add IP Group**

|                 |             |
|-----------------|-------------|
| * IP Group Name | Portal_user |
| * Start IP      | 2.2.2.1     |
| * End IP        | 2.2.2.255   |
| Service Group   | Ungrouped   |
| * Action        | Normal      |

OK Cancel

**3. Add a portal device:**

- Select **User Access Manager > Portal Service Management > Device** from the navigation tree to enter the portal device configuration page.
- Click **Add** to enter the page shown in [Figure 70](#).
- Enter the device name **NAS**.
- Enter the IP address of the router's interface connected to the host.
- Enter the key, which must be the same as that configured on the router.
- Set whether to enable IP address reallocation.  
This example uses direct portal authentication, and therefore select **No** from the **Reallocate IP** list.
- Select whether to support sever heartbeat and user heartbeat functions.  
In this example, select **Yes** for both **Support Server Heartbeat** and **Support User Heartbeat**.
- Click **OK**.

**Figure 70 Adding a portal device**

Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Add Device

---

**Add Device**

|                            |            |                          |         |
|----------------------------|------------|--------------------------|---------|
| * Device Name              | NAS        | * IP Address             | 2.2.2.1 |
| * Version                  | Portal 2.0 | * Key                    | portal  |
| * Listening Port           | 2000       | * Local Challenge        | No      |
| * Authentication Retries   | 2          | * Logout Retries         | 4       |
| * Reallocate IP            | No         | * Support User Heartbeat | Yes     |
| * Support Server Heartbeat | Yes        |                          |         |
| * Service Group            | Ungrouped  |                          |         |
| Device Description         |            |                          |         |

OK Cancel

**4. Associate the portal device with the IP address group:**

- As shown in [Figure 71](#), click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

- b. Click **Add** to enter the page shown in [Figure 72](#).
- c. Enter the port group name.
- d. Select the configured IP address group.  
The IP address used by the user to access the network must be within this IP address group.
- e. Use the default settings for other parameters.
- f. Click **OK**.

**Figure 71 Device list**

| Device Information List |            |               |            |                                                                                   |                                                                                     |                                                                                     |                                                                                     |
|-------------------------|------------|---------------|------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Add                     |            |               |            |                                                                                   |                                                                                     |                                                                                     |                                                                                     |
| 1-2 of 2. Page 1 of 1.  |            |               |            | Items per Page: 8 15 [50] 100 200                                                 |                                                                                     |                                                                                     |                                                                                     |
| Device Name             | Version    | Service Group | IP Address | Port Group Information Management                                                 | Details                                                                             | Modify                                                                              | Delete                                                                              |
| NAS                     | Portal 2.0 | Ungrouped     | 2.2.2.1    |  |  |  |  |

**Figure 72 Adding a port group**

Service >> User Access Manager >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add [Help](#)

**Port Group Info**

**Add Port Group Info**

|                             |                    |                                  |                   |
|-----------------------------|--------------------|----------------------------------|-------------------|
| * Port Group Name           | group              | * Language                       | Dynamic Detection |
| * Start Port                | 0                  | * End Port                       | zzzzz             |
| * Protocol                  | HTTP               | * Quick Authentication           | No                |
| * NAT or Not                | No                 | * Error Transparent Transmission | Yes               |
| * Authentication Type       | CHAP               | * IP Group                       | Portal_user       |
| * Heartbeat Interval        | 10                 | * Heartbeat Timeout              | 30                |
|                             | Minutes            |                                  | Minutes           |
| User Domain                 |                    | Port Group Description           |                   |
| User Attribute Type         |                    |                                  |                   |
| Default Authentication Type | Web Identity AuthN | Default Authentication Page      | index_default.jsp |

OK Cancel

5. Select **User Access Manager > Service Parameters > Validate System Configuration** from the navigation tree to validate the configurations.

## Configuring the portal server on IMC PLAT 7.1

In this example, the portal server runs on IMC PLAT 7.1 (E0303) and IMC EIA 7.1 (F0303).

1. Configure the portal authentication server:
  - a. Log in to IMC and click the **User** tab.
  - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to enter the portal server configuration page, as shown in [Figure 73](#).
  - c. Configure the portal server parameters as needed.  
This example uses the default values.
  - d. Click **OK**.

**Figure 73 Portal authentication server configuration**

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \* Info

Portal Server

Request Timeout(Seconds) \* 4 Server Heartbeat Interval(Seconds) \* 20

User Heartbeat Interval(Minutes) \* 5 LB Device Address

Portal Web

Request Timeout(Seconds) \* 15 Packet Code

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.0.111:8080/portal/

Advanced Information

Service Type List

Add

Total Items: 0.

2. Configure the IP address group:
  - a. Select **User Access Policy > Portal Service > IP Group** from the navigation tree to enter the portal IP address group configuration page.
  - b. Click **Add** to enter the page shown in [Figure 74](#).
  - c. Enter the IP group name.
  - d. Enter the start IP address and end IP address of the IP group.  
Make sure the client IP address (2.2.2.2) is in the IP group.
  - e. Select a service group.  
This example uses the default group **Ungrouped**.
  - f. Select **Normal** from the **Action** list.
  - g. Click **OK**.

**Figure 74 Adding an IP address group**

User > User Access Policy > Portal Service > IP Group > Add IP Group

Help

Add IP Group

IP Group Name \* Portal\_user

Start IP \* 2.2.2.1

End IP \* 2.2.2.255

Service Group Ungrouped

Action \* Normal

OK Cancel

3. Add a portal device:
  - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to enter the portal device configuration page.
  - b. Click **Add** to enter the page shown in [Figure 75](#).
  - c. Enter the device name.
  - d. Enter the IP address of the router's interface that exchanges information with the portal server.
  - e. Set whether to support the portal server heartbeat and user heartbeat functions.  
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
  - f. Enter the key, which must be the same as that configured on the router.
  - g. Select **Directly Connected** from the **Access Method** list.
  - h. Click **OK**.

**Figure 75 Adding a portal device**

User > User Access Policy > Portal Service > Device > Add Device

Help

Add Device

Device Information

Device Name \* NAS

Version \* Portal 2.0

Listening Port \* 2000

Authentication Retries \* 0

Support Server Heartbeat \* No

Key \* .....

Access Method \* Directly Connected

Device Description

Service Group \* Ungrouped

IP Address \* 2.2.2.1

Local Challenge \* No

Logout Retries \* 1

Support User Heartbeat \* No

Confirm Key \* .....

OK Cancel

4. Associate the portal device with the IP address group:
  - a. As shown in Figure 76, click the **Port Group Information Management** icon for device **NAS** to enter the port group configuration page.
  - b. Click **Add** to enter the page shown in Figure 77.
  - c. Enter the port group name.
  - d. Select the configured IP address group.
 

The IP address used by the user to access the network must be within this IP address group.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 76 Device list**

User > User Access Policy > Portal Service > Device

★ Add to My Favorites ? Help

Query Devices

Device Name  Version

Deploy Result  Service Group

| Device Name | Version    | Service Group | IP Address | Last Deployed at | Deploy Result | Operation                                                                                                                                                                                                                                                                                                                                           |
|-------------|------------|---------------|------------|------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAS         | Portal 2.0 | Ungrouped     | 2.2.2.1    |                  | Not Deployed  |     |

1-1 of 1. Page 1 of 1.

« < 1 > » 50

**Figure 77 Adding a port group**

## Configuring the router

1. Configure a RADIUS scheme:
 

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Router> system-view
[Router] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Router-radius-rs1] primary authentication 192.168.0.112
```

```
[Router-radius-rs1] primary accounting 192.168.0.112
```

```
[Router-radius-rs1] key authentication simple radius
```

```
[Router-radius-rs1] key accounting simple radius
```

# Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Router-radius-rs1] user-name-format without-domain
```

```
[Router-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Router] radius session-control enable
```

## 2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[Router] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[Router-isp-dm1] authentication portal radius-scheme rs1
```

```
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
```

```
[Router-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Router] domain default enable dm1
```

## 3. Configure portal authentication:

# Configure a portal authentication server.

```
[Router] portal server newpt
```

```
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[Router-portal-server-newpt] port 50100
```

# Configure reachability detection of the portal authentication server: set the server detection interval to 40 seconds, and send log messages upon reachability status changes.

```
[Router-portal-server-newpt] server-detect timeout 40 log
```

---

### NOTE:

The value of **timeout** must be greater than or equal to the portal server heartbeat interval.

---

# Configure portal user synchronization with the portal authentication server, and set the synchronization detection interval to 600 seconds.

```
[Router-portal-server-newpt] user-sync timeout 600
```

```
[Router-portal-server-newpt] quit
```

---

### NOTE:

The value of **timeout** must be greater than or equal to the portal user heartbeat interval.

---

# Configure a portal Web server.

```
[Router] portal web-server newpt
```

```
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[Router-portal-websvr-newpt] quit
```

# Enable direct portal authentication on GigabitEthernet 2/0/2.

```
[Router] interface gigabitethernet 2/0/2
```

```

[Router-GigabitEthernet2/0/2] portal enable method direct
Enable portal fail-permit for the portal authentication server newpt.
[Router-GigabitEthernet2/0/2] portal fail-permit server newpt
Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
Configure the BAS-IP as 2.2.2.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 2.2.2.1
[Router-GigabitEthernet2/0/2] quit

```

## Verifying the configuration

# Use the following command to display information about the portal authentication server.

```
[Router] display portal server newpt
```

Portal server: newpt

```

IP : 192.168.0.111
VPN instance : Not configured
Port : 50100
Server Detection : Timeout 40s Action: log
User synchronization : Timeout 600s
Status : Up

```

The **Up** status of the portal authentication server indicates that the portal authentication server is reachable. If the access device detects that the portal authentication server is unreachable, the **Status** field in the command output displays **Down**. The access device generates a server unreachable log "Portal server newpt turns down from up." and disables portal authentication on the access interface, so the host can access the external network without authentication.

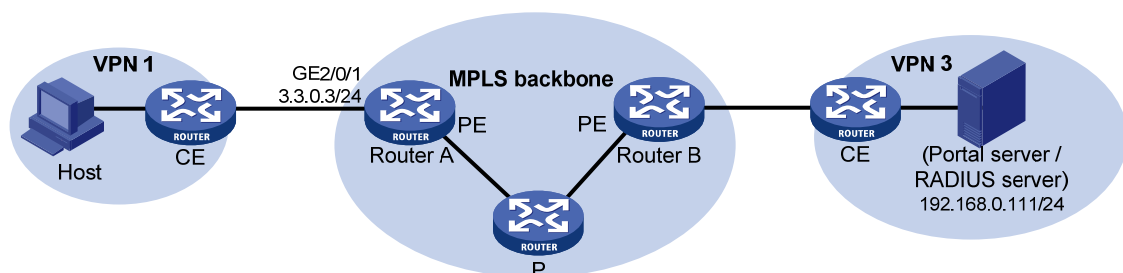
# Configuring cross-subnet portal authentication for MPLS L3VPNs

## Network requirements

As shown in [Figure 78](#), the PE device Router A provides portal authentication for the host in VPN 1. A portal server in VPN 3 acts as the portal authentication server, portal Web server, and RADIUS server.

Configure cross-subnet portal authentication on Router A, so the host can access Internet resources after passing identity authentication.

**Figure 78 Network diagram**



## Configuration prerequisites

- Before enabling portal authentication, configure MPLS L3VPN and specify VPN targets for VPN 1 and VPN 3 so that VPN 1 and VPN 3 can communicate with each other. This example

describes only the access authentication configuration on the user-side PE. For information about MPLS L3VPN configurations, see *MPLS Configuration Guide*.

- Configure the RADIUS server correctly to provide authentication and accounting functions.

## Configuration procedure

Perform the following tasks on Router A.

### 1. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1** and enter its view.

```
<RouterA> system-view
```

```
[RouterA] radius scheme rs1
```

# For the RADIUS scheme, specify the VPN instance that is bound to the interface connected to the portal/RADIUS server. This example uses VPN instance **vpn3**.

```
[RouterA-radius-rs1] vpn-instance vpn3
```

---

#### NOTE:

For the VPN instance information, see the MPLS L3VPN configuration on Router A.

---

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[RouterA-radius-rs1] primary authentication 192.168.0.111
```

```
[RouterA-radius-rs1] primary accounting 192.168.0.111
```

```
[RouterA-radius-rs1] key accounting simple radius
```

```
[RouterA-radius-rs1] key authentication simple radius
```

# Exclude the ISP domain name from the username sent to the RADIUS server.

```
[RouterA-radius-rs1] user-name-format without-domain
```

# Specify the source IP address for RADIUS packets to be sent as 3.3.0.3. This address must be the same as that of the portal device specified on the portal authentication server to avoid authentication failures.

```
[RouterA-radius-rs1] nas-ip 3.3.0.3
```

```
[RouterA-radius-rs1] quit
```

# Enable RADIUS session control.

```
[RouterA] radius session-control enable
```

### 2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[RouterA] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
```

```
[RouterA-isp-dm1] authorization portal radius-scheme rs1
```

```
[RouterA-isp-dm1] accounting portal radius-scheme rs1
```

```
[RouterA-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[RouterA] domain default enable dm1
```

### 3. Configure portal authentication:

# Configure a portal authentication server.

```
[RouterA] portal server newpt
```

```
[RouterA-portal-server-newpt] ip 192.168.0.111 vpn-instance vpn3 key simple portal
```

```
[RouterA-portal-server-newpt] port 50100
```



```

[RouterA-portal-server-newpt] quit
Configure a portal Web server.
[RouterA] portal web-server newpt
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[RouterA-portal-websvr-newpt] vpn-instance vpn3
[RouterA-portal-websvr-newpt] quit
Enable cross-subnet portal authentication on GigabitEthernet 2/0/1.
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] portal enable method layer3
Reference the portal Web server newpt on GigabitEthernet 2/0/1.
[RouterA-GigabitEthernet2/0/1] portal apply web-server newpt
Configure the BAS-IP as 3.3.0.3 for portal packets sent from GigabitEthernet 2/0/1 to the
portal authentication server.
[RouterA-GigabitEthernet2/0/1] portal bas-ip 3.3.0.3
[RouterA-GigabitEthernet2/0/1] quit

```

## Verifying the configuration

# Verify the portal configuration by executing the **display portal interface** command. (Details not shown.)

# After the user passes authentication, execute the **display portal user** command to display the portal user information.

```

[RouterA] display portal user all
Total portal users: 1
Username: abc
 Portal server: newpt
 State: Online
 VPN instance: vpn3
 MAC IP VLAN Interface
 000d-88f7-c268 3.3.0.1 -- GigabitEthernet2/0/1
Authorization information:
 DHCP IP pool: N/A
 Session group profile: N/A
 ACL: N/A
 CAR: N/A

```

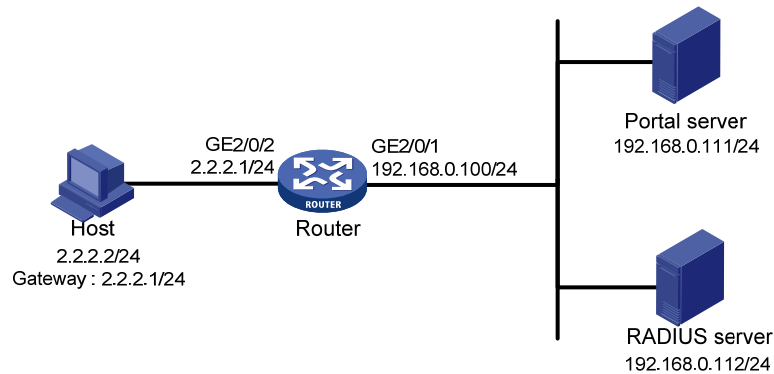
## Configuring direct portal authentication with a preauthentication domain

### Network requirements

As shown in [Figure 79](#), the host is directly connected to the router (the access device). The host is assigned with a public IP address through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication, so the host can access only subnet 192.168.0.0/24 before passing the authentication and access other network resources after passing the authentication.

Figure 79 Network diagram



### Configuration prerequisites

- Configure IP addresses for the host, router, and servers as shown in [Figure 79](#) and make sure they can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.

### Configuration procedure

Perform the following tasks on the router.

1. Configure a preauthentication IP address pool:  
# Configure DHCP address pool **pre** to assign IP addresses and other configuration parameters to clients on subnet 2.2.2.0/24.  

```
<Router> system-view
[Router] dhcp server ip-pool pre
[Router-dhcp-pool-pre] gateway-list 2.2.2.1
[Router-dhcp-pool-pre] network 2.2.2.0 24
[Router-dhcp-pool-pre] quit
```

  
# Enable the DHCP server on GigabitEthernet 2/0/2.  

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] dhcp select server
[Router-GigabitEthernet2/0/2] quit
```
2. Configure a preauthentication domain:  
# Create an ISP domain named **abc** and enter its view.  

```
[Router] domain abc
```

  
# Specify authorization ACL 3010 in the domain.  

```
[Router-isp-abc] authorization-attribute acl 3010
[Router-isp-abc] quit
```

  
# Configure a rule to permit access to the subnet 192.168.0.0/24.  

```
[Router] acl advanced 3010
[Router-acl-ipv4-adv-3010] rule 1 permit ip destination 192.168.0.0 24
[Router-acl-ipv4-adv-3010] quit
```

  
# Configure preauthentication domain **abc** on GigabitEthernet 2/0/2.  

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal pre-auth domain abc
[Router-GigabitEthernet2/0/2] quit
```
3. Configure portal authentication:  
# Configure a portal authentication server.

```

[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
Configure a portal Web server.
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
Enable direct portal authentication on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal enable method direct
Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
Configure the BAS-IP as 2.2.2.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 2.2.2.1
[Router-GigabitEthernet2/0/2] quit

```

## Verifying the configuration

# Verify the portal configuration by executing the **display portal interface** command. (Details not shown.)

# Display information about preauthentication portal users.

```
[Router] display portal user pre-auth interface gigabitethernet 2/0/2
```

| MAC            | IP      | VLAN | Interface            |
|----------------|---------|------|----------------------|
| 0015-e9a6-7cfe | 2.2.2.4 | --   | GigabitEthernet2/0/2 |

State: Online

VPN instance: --

Authorization information:

DHCP IP pool: N/A

Session group profile: N/A

ACL number: 3010

Inbound CAR: N/A

Outbound CAR: N/A

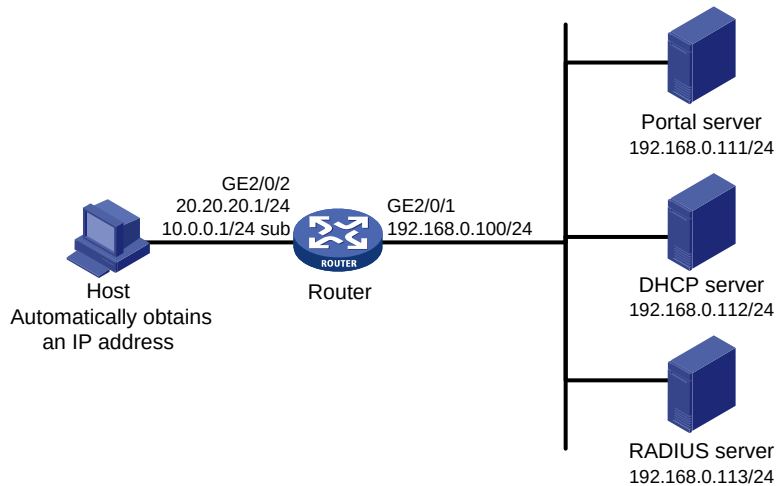
## Configuring re-DHCP portal authentication with a preauthentication domain

### Network requirements

As shown in [Figure 80](#), the host is directly connected to the router (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure re-DHCP portal authentication. Before passing the authentication, the host is assigned a private IP address and can access only the subnet 192.168.0.0/24. After passing the authentication, the host gets a public IP address and can access other network resources.

Figure 80 Network diagram



### Configuration prerequisites and guidelines

- Configure IP addresses for the router and servers as shown in [Figure 80](#) and make sure the host, router, and servers can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
  - The router must be configured as a DHCP relay agent.
  - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).

For information about DHCP relay agent configuration, see *Layer 3—IP Services Configuration Guide*.

- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the router's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.
- If you have configured a preauthentication IP address pool on portal-enabled interfaces, configure a DHCP relay address pool with the same name on the device. For the DHCP relay address pool, specify the subnet address the unauthenticated users reside (with the **export-router** keyword specified) and the DHCP server address.

### Configuration procedure

Perform the following tasks on the router.

1. Configure a preauthentication domain:
  - # Create an ISP domain named **abc** and enter its view.

```
<Router> system-view
[Router] domain abc
```
  - # Specify authorization ACL 3010 in the domain.

```
[Router-isp-abc] authorization-attribute acl 3010
[Router-isp-abc] quit
```
  - # Configure a rule to permit access to the subnet 192.168.0.0/24.

```
[Router] acl advanced 3010
```

```

[Router-acl-ipv4-adv-3010] rule 1 permit ip destination 192.168.0.0 24
[Router-acl-ipv4-adv-3010] quit
Configure preauthentication domain abc on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal pre-auth domain abc
[Router-GigabitEthernet2/0/2] quit
2. Configure DHCP relay and authorized ARP.
Configure DHCP relay.
[Router] dhcp enable
[Router] dhcp relay client-information record
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] ip address 20.20.20.1 255.255.255.0
[Router-GigabitEthernet2/0/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet2/0/2] dhcp select relay
[Router-GigabitEthernet2/0/2] dhcp relay server-address 192.168.0.112
Enable authorized ARP.
[Router-GigabitEthernet2/0/2] arp authorized enable
[Router-GigabitEthernet2/0/2] quit
3. Configure portal authentication:
Configure a portal authentication server.
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
Configure a portal Web server.
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
Enable re-DHCP portal authentication on GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] portal enable method redhcp
Reference the portal Web server newpt on GigabitEthernet 2/0/2.
[Router-GigabitEthernet2/0/2] portal apply web-server newpt
Configure the BAS-IP as 20.20.20.1 for portal packets sent from GigabitEthernet 2/0/2 to the
portal authentication server.
[Router-GigabitEthernet2/0/2] portal bas-ip 20.20.20.1
[Router-GigabitEthernet2/0/2] quit

```

## Verifying the configuration

```

Verify the portal configuration by executing the display portal interface command. (Details not
shown.)

Display information about preauthentication portal users.
[Router] display portal user pre-auth interface gigabitethernet 2/0/2
MAC IP VLAN Interface
0015-e9a6-7cfe 10.10.10.4 -- GigabitEthernet2/0/2
State: Online
VPN instance: --
DHCP IP pool: N/A

```

Session group profile: N/A  
ACL number: 3010  
Inbound CAR: N/A  
Outbound CAR: N/A

# Troubleshooting portal

## No portal authentication page is pushed for users

### Symptom

When a user is redirected to the IMC portal authentication server, no portal authentication page or error message is prompted for the user. The login page is blank.

### Analysis

The key configured on the portal access device and that configured on the portal authentication server are inconsistent. As a result, packet verification fails, and the portal authentication server refuses to push the authentication page.

### Solution

Use the **display portal server** command on the access device to check whether a key is configured for the portal authentication server.

- If no key is configured, configure the right key.
- If a key is configured, use the **ip** or **ipv6** command in the portal authentication server view to correct the key, or correct the key configured for the access device on the portal authentication server.

## Cannot log out portal users on the access device

### Symptom

You cannot use the **portal delete-user** command on the access device to log out a portal user, but the portal user can log out by clicking the **Disconnect** button on the portal authentication client.

### Analysis

When you execute the **portal delete-user** command on the access device to log out a user, the access device sends an unsolicited logout notification message to the portal authentication server. The destination port number in the logout notification is the listening port number of the portal authentication server configured on the access device. If this listening port number is not the actual listening port number configured on the server, the server cannot receive the notification. As a result, the server does not log out the user.

When a user uses the **Disconnect** button on the authentication client to log out, the portal authentication server sends an unsolicited logout request message to the access device. The access device uses the source port in the logout request as the destination port in the logout ACK message. As a result, the portal authentication server can definitely receive the logout ACK message and log out the user.

### Solution

1. Use the **display portal server** command to display the listening port of the portal authentication server configured on the access device.
2. Use the **portal server** command in system view to change the listening port number to the actual listening port of the portal authentication server.

# Cannot log out portal users on the RADIUS server

## Symptom

The access device uses the HPE IMC server as the RADIUS server to perform identity authentication for portal users. You cannot log out the portal users on the RADIUS server.

## Analysis

The HPE IMC server uses session control packets to send disconnection requests to the access device. On the access device, the listening UDP port for session control packets is disabled by default. Therefore, the access device cannot receive the portal user logout requests from the RADIUS server.

## Solution

On the access device, execute the **radius session-control enable** command in system view to enable the RADIUS session control function.

# Users logged out by the access device still exist on the portal authentication server

## Symptom

After you log out a portal user on the access device, the user still exists on the portal authentication server.

## Analysis

When you execute the **portal delete-user** command on the access device to log out a user, the access device sends an unsolicited logout notification to the portal authentication server. If the BAS-IP or BAS-IPv6 address carried in the logout notification is different from the portal device IP address specified on the portal authentication server, the portal authentication server discards the logout notification. When sending of the logout notifications times out, the access device logs out the user. However, the portal authentication server does not receive the logout notification successfully, and therefore it regards the user is still online.

## Solution

Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.

# Re-DHCP portal authenticated users cannot log in successfully

## Symptom

The device performs re-DHCP portal authentication for users. A user enters the correct username and password, and the client successfully obtains the private and public IP addresses. However, the authentication result for the user is failure.

## Analysis

When the access device detects that the client IP address is changed, it sends an unsolicited portal packet to notify of the IP change to the portal authentication server. The portal authentication server notifies of the authentication success only after it receives the IP change notification from both the access device and the client.

If the BAS-IP or BAS-IPv6 address carried in the portal notification packet is different from the portal device IP address specified on the portal authentication server, the portal authentication server

discards the portal notification packet. As a result, the portal authentication server considers that the user has failed the authentication.

### **Solution**

Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.



# Configuring port security

## Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. This feature applies to networks, such as a WLAN, that require different authentication methods for different users on a port.

Port security provides the following functions:

- Prevents unauthorized access to a network by checking the source MAC address of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC address of outbound traffic.
- Controls MAC address learning and authentication on a port to make sure the port learns only source trusted MAC addresses.

A frame is illegal if its source MAC address cannot be learned in a port security mode or it is from a client that has failed 802.1X or MAC authentication. The port security feature automatically takes a predefined action on illegal frames. This automatic mechanism enhances network security and reduces human intervention.

---

**NOTE:**

As a best practice, use the 802.1X authentication or MAC authentication feature rather than port security for scenarios that require only 802.1X authentication or MAC authentication. For more information about 802.1X and MAC authentication, see "[Configuring 802.1X](#)" and "[Configuring MAC authentication](#)."

---

## Port security features

### NTK

The need to know (NTK) feature prevents traffic interception by checking the destination MAC address in the outbound frames. The feature ensures that frames are sent only to the following hosts:

- Hosts that have passed authentication.
- Hosts whose MAC addresses have been learned or configured on the access device.

### Intrusion protection

The intrusion protection feature checks the source MAC address in inbound frames for illegal frames, and takes a predefined action on each detected illegal frame. The action can be disabling the port temporarily, disabling the port permanently, or blocking frames from the illegal MAC address for 3 minutes (not user configurable).

## Port security modes

Port security supports the following categories of security modes:

- **MAC learning control**—Includes two modes: autoLearn and secure. MAC address learning is permitted on a port in autoLearn mode and disabled in secure mode.
- **Authentication**—Security modes in this category implement MAC authentication, 802.1X authentication, or a combination of these two authentication methods.

Upon receiving a frame, the port in a security mode searches the MAC address table for the source MAC address. If a match is found, the port forwards the frame. If no match is found, the port learns the MAC address or performs authentication, depending on the security mode. If the frame is illegal, the port takes the predefined NTK or intrusion protection action. Outgoing frames are not restricted by port security's NTK action unless they trigger the NTK feature.

The maximum number of users a port supports equals the smaller value from the following values:

- The maximum number of secure MAC addresses that port security allows.
- The maximum number of concurrent users the authentication mode in use allows.

For example, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode, port security's limit takes effect.

Table 8 describes the port security modes and the security features.

**Table 8 Port security modes**

| Purpose                                                                  | Security mode                                                                                                                      |                                  | Features that can be triggered |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------------------------|
| Turning off the port security feature                                    | noRestrictions (the default mode)<br>In this mode, port security is disabled on the port and access to the port is not restricted. |                                  | N/A                            |
| Controlling MAC address learning                                         | autoLearn                                                                                                                          |                                  | NTK/intrusion protection       |
|                                                                          | secure                                                                                                                             |                                  |                                |
| Performing 802.1X authentication                                         | userLogin                                                                                                                          |                                  | N/A                            |
|                                                                          | userLoginSecure                                                                                                                    |                                  | NTK/intrusion protection       |
|                                                                          | userLoginSecureExt                                                                                                                 |                                  |                                |
|                                                                          | userLoginWithOUI                                                                                                                   |                                  |                                |
| Performing MAC authentication                                            | macAddressWithRadius                                                                                                               |                                  | NTK/intrusion protection       |
| Performing a combination of MAC authentication and 802.1X authentication | Or                                                                                                                                 | macAddressOrUserLoginSecure      | NTK/intrusion protection       |
|                                                                          |                                                                                                                                    | macAddressOrUserLoginSecureExt   |                                |
|                                                                          | Else                                                                                                                               | macAddressElseUserLoginSecure    |                                |
|                                                                          |                                                                                                                                    | macAddressElseUserLoginSecureExt |                                |



**TIP:**

- **userLogin** specifies 802.1X authentication and port-based access control. **userLogin** with **Secure** specifies 802.1X authentication and MAC-based access control. **Ext** indicates allowing multiple 802.1X users to be authenticated and serviced at the same time. A security mode without **Ext** allows only one user to pass 802.1X authentication.
- **macAddress** specifies MAC authentication.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, whether to turn to the authentication method following **Else** depends on the protocol type of the authentication request.
- **Or** specifies that the authentication method following **Or** is applied first. If the authentication fails, the authentication method before **Or** is applied.

## Controlling MAC address learning

- autoLearn.

A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, these MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command.

A port in autoLearn mode allows frames sourced from the following MAC addresses to pass:

- Secure MAC addresses.
- MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands.

When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.

- secure.

MAC address learning is disabled on a port in secure mode. You configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. For more information about configuring MAC address table entries, see *Layer 2—LAN Switching Configuration Guide*.

A port in secure mode allows only frames sourced from the following MAC addresses to pass:

- Secure MAC addresses.
- MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands.

## Performing 802.1X authentication

- userLogin.

A port in this mode performs 802.1X authentication and implements port-based access control. The port can service multiple 802.1X users. Once an 802.1X user passes authentication on the port, any subsequent 802.1X users can access the network through the port without authentication.

- userLoginSecure.

A port in this mode performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.

- userLoginSecureExt.

This mode is similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.

- userLoginWithOUI.

This mode is similar to the userLoginSecure mode. The difference is that a port in this mode also permits frames from one user whose MAC address contains a specific OUI.

In this mode, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

---

### NOTE:

An OUI is a 24-bit number that uniquely identifies a vendor, manufacturer, or organization. In MAC addresses, the first three octets are the OUI.

---

## Performing MAC authentication

macAddressWithRadius: A port in this mode performs MAC authentication, and services multiple users.

## Performing a combination of MAC authentication and 802.1X authentication

- macAddressOrUserLoginSecure.

This mode is the combination of the macAddressWithRadius and userLoginSecure modes. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

In this mode, the port performs 802.1X authentication first. If 802.1X authentication fails, MAC authentication is performed.

- `macAddressOrUserLoginSecureExt`.

This mode is similar to the `macAddressOrUserLoginSecure` mode, except that this mode supports multiple 802.1X and MAC authentication users.

- `macAddressElseUserLoginSecure`.

This mode is the combination of the `macAddressWithRadius` and `userLoginSecure` modes, with MAC authentication having a higher priority as the **Else** keyword implies. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.

In this mode, the port performs MAC authentication upon receiving non-802.1X frames. Upon receiving 802.1X frames, the port performs MAC authentication and then, if the authentication fails, 802.1X authentication.

- `macAddressElseUserLoginSecureExt`.

This mode is similar to the `macAddressElseUserLoginSecure` mode except that this mode supports multiple 802.1X and MAC authentication users as the **Ext** keyword implies.

## Feature and hardware compatibility

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

## Configuration task list

| Tasks at a glance                                                                                                                                                                                            | Remarks                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| (Required.) <a href="#">Enabling port security</a>                                                                                                                                                           | N/A                                                                                 |
| (Optional.) <a href="#">Setting port security's limit on the number of secure MAC addresses on a port</a>                                                                                                    | N/A                                                                                 |
| (Required.) <a href="#">Setting the port security mode</a>                                                                                                                                                   | N/A                                                                                 |
| (Required.) <a href="#">Configuring port security features:</a> <ul style="list-style-type: none"><li>• <a href="#">Configuring NTK</a></li><li>• <a href="#">Configuring intrusion protection</a></li></ul> | Configure one or more port security features according to the network requirements. |
| (Optional.) <a href="#">Configuring secure MAC addresses</a>                                                                                                                                                 | N/A                                                                                 |
| (Optional.) <a href="#">Ignoring authorization information from the server</a>                                                                                                                               | N/A                                                                                 |
| (Optional.) <a href="#">Enabling MAC move</a>                                                                                                                                                                | N/A                                                                                 |
| (Optional.) <a href="#">Enabling the authorization-fail-offline feature</a>                                                                                                                                  | N/A                                                                                 |
| (Optional.) <a href="#">Applying a NAS-ID profile to port security</a>                                                                                                                                       | N/A                                                                                 |

## Enabling port security

Before you enable port security, disable 802.1X and MAC authentication globally.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. Port security automatically modifies these settings in different security modes.

To enable port security:

| Step                     | Command                     | Remarks                                |
|--------------------------|-----------------------------|----------------------------------------|
| 1. Enter system view.    | <b>system-view</b>          | N/A                                    |
| 2. Enable port security. | <b>port-security enable</b> | By default, port security is disabled. |

You can use the **undo port-security enable** command to disable port security. Because the command logs off the online users, make sure no online users are present.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based.
- Port authorization state is auto.

For more information about 802.1X authentication and MAC authentication configuration, see "[Configuring 802.1X](#)" and "[Configuring MAC authentication](#)."

## Setting port security's limit on the number of secure MAC addresses on a port

You can set the maximum number of secure MAC addresses that port security allows on a port for the following purposes:

- Controlling the number of concurrent users on the port.  
For a port operating in a security mode (except for autoLearn and secure), the upper limit equals the smaller of the following values:
  - The limit of the secure MAC addresses that port security allows.
  - The limit of concurrent users allowed by the authentication mode in use.
- Controlling the number of secure MAC addresses on the port in autoLearn mode.

The port security's limit on the number of secure MAC addresses on a port is independent of the MAC learning limit described in MAC address table configuration. For more information about MAC address table configuration, see *Layer 2—LAN Switching Configuration Guide*.

To set the maximum number of secure MAC addresses allowed on a port:

| Step                                                                 | Command                                                           | Remarks                                                                                |
|----------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                | N/A                                                                                    |
| 2. Enter Layer 2 Ethernet interface view.                            | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                                                                    |
| 3. Set the maximum number of secure MAC addresses allowed on a port. | <b>port-security max-mac-count</b><br><i>count-value</i>          | By default, port security does not limit the number of secure MAC addresses on a port. |

## Setting the port security mode

Port security modes except the userLogin mode are supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:

- HMIM-8GSW.
- HMIM-24GSW.
- HMIM-24GSWP.
- SIC-4GSW.
- SIC-4GSWP.
- Fixed Layer 2 Ethernet ports on the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

Before you set a port security mode for a port, complete the following tasks:

- Disable 802.1X and MAC authentication.
- Verify that the port does not belong to any aggregation group or service loopback group.
- If you are configuring the autoLearn mode, set port security's limit on the number of secure MAC addresses. You cannot change the setting when the port is operating in autoLearn mode.

When you set the port security mode, follow these guidelines:

- You can specify a port security mode when port security is disabled, but your configuration cannot take effect.
- Changing the port security mode of a port logs off the online users of the port.
- Do not enable 802.1X authentication or MAC authentication on a port where port security is configured.

To set the port security mode:

| Step                                                     | Command                                                                                                                                                                                                                                                                                                                                                  | Remarks                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                    | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                       | N/A                                                                                                                                                                                                                                                                                                                                                                                |
| 2. (Optional.) Set an OUI value for user authentication. | <b>port-security oui index</b><br><i>index-value mac-address</i><br><i>oui-value</i>                                                                                                                                                                                                                                                                     | By default, no OUI value is configured for user authentication.<br><br>This command is required for the <b>userlogin-withoui</b> mode.<br><br>You can set multiple OUIs, but when the port security mode is <b>userlogin-withoui</b> , the port allows one 802.1X user and only one user that matches one of the specified OUIs.                                                   |
| 3. Enter interface view.                                 | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                                                                                                                                                                        | N/A                                                                                                                                                                                                                                                                                                                                                                                |
| 4. Set the port security mode.                           | <b>port-security port-mode</b><br>{ <b>autolearn</b>   <b>mac-authentication</b>   <b>mac-else-userlogin-secure</b>   <b>mac-else-userlogin-secure-ext</b>   <b>secure</b>   <b>userlogin</b>   <b>userlogin-secure</b>   <b>userlogin-secure-ext</b>   <b>userlogin-secure-or-mac</b>   <b>userlogin-secure-or-mac-ext</b>   <b>userlogin-withoui</b> } | By default, a port operates in noRestrictions mode.<br><br>After enabling port security, you can change the port security mode of a port only when the port is operating in noRestrictions (the default) mode. To change the port security mode for a port in any other mode, first use the <b>undo port-security port-mode</b> command to restore the default port security mode. |

# Configuring port security features

Port security features are supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
  - HMIM-8GSW.
  - HMIM-24GSW.
  - HMIM-24GSWP.
  - SIC-4GSW.
  - SIC-4GSWP.
- Fixed Layer 2 Ethernet ports on the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

## Configuring NTK

The NTK feature checks the destination MAC addresses in outbound frames to make sure frames are forwarded only to authenticated devices.

The NTK feature supports the following modes:

- **ntkonly**—Forwards only unicast frames with authenticated destination MAC addresses.
- **ntk-withbroadcasts**—Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.
- **ntk-withmulticasts**—Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

The NTK feature drops any unicast frame with an unknown destination MAC address. Not all port security modes support triggering the NTK feature. For more information, see [Table 8](#).

To configure the NTK feature:

| Step                                      | Command                                                                                                        | Remarks                                                                      |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 1. Enter system view.                     | <b>system-view</b>                                                                                             | N/A                                                                          |
| 2. Enter Layer 2 Ethernet interface view. | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                              | N/A                                                                          |
| 3. Configure the NTK feature.             | <b>port-security ntk-mode</b><br>{ <b>ntk-withbroadcasts</b>  <br><b>ntk-withmulticasts</b>   <b>ntkonly</b> } | By default, NTK is disabled on a port and all frames are allowed to be sent. |

## Configuring intrusion protection

Intrusion protection enables a device to take one of the following actions in response to illegal frames:

- **blockmac**—Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards the frames. All subsequent frames sourced from a blocked MAC address are dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is fixed and cannot be changed.
- **disableport**—Disables the port until you bring it up manually.

- **disableport-temporarily**—Disables the port for a period of time. The period can be configured with the **port-security timer disableport** command.

To configure the intrusion protection feature:

| Step                                                                                | Command                                                                                                          | Remarks                                             |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| 1. Enter system view.                                                               | <b>system-view</b>                                                                                               | N/A                                                 |
| 2. Enter Layer 2 Ethernet interface view.                                           | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                | N/A                                                 |
| 3. Configure the intrusion protection feature.                                      | <b>port-security intrusion-mode</b><br>{ <b>blockmac</b>   <b>disableport</b>   <b>disableport-temporarily</b> } | By default, intrusion protection is disabled.       |
| 4. Return to system view.                                                           | <b>quit</b>                                                                                                      | N/A                                                 |
| 5. (Optional.) Set the silence timeout period during which a port remains disabled. | <b>port-security timer disableport</b><br><i>time-value</i>                                                      | By default, the port silence timeout is 20 seconds. |

**NOTE:**

On a port operating in either `macAddressElseUserLoginSecure` mode or `macAddressElseUserLoginSecureExt` mode, intrusion protection is triggered only after both MAC authentication and 802.1X authentication fail for the same frame.

## Configuring secure MAC addresses

Secure MAC addresses are configured or learned in `autoLearn` mode. If the secure MAC addresses are saved, they can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.

Secure MAC addresses include static, sticky, and dynamic secure MAC addresses.

**Table 9 Comparison of static, sticky, and dynamic secure MAC addresses**

| Type   | Address sources                                                                                                    | Aging mechanism                                                                                                                                                                                                                                                                                 | Can be saved and survive a device reboot? |
|--------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Static | Manually added (by using the <b>port-security mac-address security</b> command without the <b>sticky</b> keyword). | Not available.<br>The static secure MAC addresses never age out unless you perform any of the following tasks: <ul style="list-style-type: none"> <li>• Manually remove these MAC addresses.</li> <li>• Change the port security mode.</li> <li>• Disable the port security feature.</li> </ul> | Yes.                                      |



| Type    | Address sources                                                                                                                                                                                                                                                                                         | Aging mechanism                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Can be saved and survive a device reboot?                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Sticky  | <ul style="list-style-type: none"> <li>Manually added (by using the <b>port-security mac-address security</b> command with the <b>sticky</b> keyword).</li> <li>Converted from dynamic secure MAC addresses.</li> <li>Automatically learned when the dynamic secure MAC feature is disabled.</li> </ul> | <p>By default, sticky MAC addresses do not age out. However, you can configure an aging timer or use the aging timer together with the inactivity aging feature to remove old sticky MAC addresses.</p> <ul style="list-style-type: none"> <li>If only the aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC addresses.</li> <li>If both the aging timer and the inactivity aging feature are configured, the aging timer restarts once traffic data is detected from the sticky MAC addresses.</li> </ul> | <p>Yes.</p> <p>The secure MAC aging timer restarts at a reboot.</p>    |
| Dynamic | <ul style="list-style-type: none"> <li>Converted from sticky MAC addresses.</li> <li>Automatically learned after the dynamic secure MAC feature is enabled.</li> </ul>                                                                                                                                  | Same as sticky MAC addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>No.</p> <p>All dynamic secure MAC addresses are lost at reboot.</p> |

When the maximum number of secure MAC address entries is reached, the port changes to secure mode. In secure mode, the port cannot add or learn any more secure MAC addresses. The port allows only frames sourced from secure MAC addresses or MAC addresses configured by using the **mac-address dynamic** or **mac-address static** command to pass through.

## Configuration prerequisites

Before you configure secure MAC addresses, complete the following tasks:

- Enable port security.
- Set port security's limit on the number of MAC addresses on the port. Perform this task before you enable autoLearn mode.
- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

## Configuration procedure

To configure a secure MAC address:

| Step                                           | Command                                                         | Remarks                                          |
|------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------|
| 1. Enter system view.                          | <b>system-view</b>                                              | N/A                                              |
| 2. (Optional.) Set the secure MAC aging timer. | <b>port-security timer autolearn aging</b><br><i>time-value</i> | By default, secure MAC addresses do not age out. |

| Step                                                  | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Remarks                                                                                                                                                            |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Configure a secure MAC address.                    | <ul style="list-style-type: none"> <li>In system view:<br/> <b>port-security mac-address security [ sticky ] mac-address interface interface-type interface-number vlan vlan-id</b> </li> <li>In Layer 2 Ethernet interface view: <ul style="list-style-type: none"> <li>a. <b>interface interface-type interface-number</b></li> <li>b. <b>port-security mac-address security [ sticky ] mac-address vlan vlan-id</b></li> <li>c. <b>quit</b></li> </ul> </li> </ul> | <p>By default, no secure MAC address exists.</p> <p>In a VLAN, a MAC address cannot be specified as both a static secure MAC address and a sticky MAC address.</p> |
| 4. Enter Layer 2 Ethernet interface view.             | <b>interface interface-type interface-number</b>                                                                                                                                                                                                                                                                                                                                                                                                                      | N/A                                                                                                                                                                |
| 5. (Optional.) Enable inactivity aging.               | <b>port-security mac-address aging-type inactivity</b>                                                                                                                                                                                                                                                                                                                                                                                                                | By default, the inactivity aging feature is disabled.                                                                                                              |
| 6. (Optional.) Enable the dynamic secure MAC feature. | <b>port-security mac-address dynamic</b>                                                                                                                                                                                                                                                                                                                                                                                                                              | By default, the dynamic secure MAC feature is disabled. Sticky MAC addresses can be saved to the configuration file. Once saved, they can survive a device reboot. |

## Ignoring authorization information from the server

You can configure a port to ignore the authorization information received from the server (local or remote) after an 802.1X or MAC authentication user passes authentication.

To configure a port to ignore authorization information from the server:

| Step                                                                             | Command                                          | Remarks                                                                                        |
|----------------------------------------------------------------------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                            | <b>system-view</b>                               | N/A                                                                                            |
| 2. Enter Layer 2 Ethernet interface view.                                        | <b>interface interface-type interface-number</b> | N/A                                                                                            |
| 3. Ignore the authorization information received from the authentication server. | <b>port-security authorization ignore</b>        | By default, a port uses the authorization information received from the authentication server. |

## Enabling MAC move

MAC move allows 802.1X or MAC authenticated users to move between ports on a device. For example, if an authenticated 802.1X user moves to another 802.1X-enabled port on the device, the authentication session is deleted from the first port. The user is reauthenticated on the new port.

If MAC move is disabled and an 802.1X authenticated user moves to another port, the user is not reauthenticated.

As a best practice, enable MAC move for wireless users that roam between ports to access the network.

To enable MAC move:

| Step                  | Command                              | Remarks                           |
|-----------------------|--------------------------------------|-----------------------------------|
| 1. Enter system view. | <b>system-view</b>                   | N/A                               |
| 2. Enable MAC move.   | <b>port-security mac-move permit</b> | By default, MAC move is disabled. |

## Enabling the authorization-fail-offline feature

The authorization-fail-offline feature logs off port security users who fail ACL authorization.

A user fails ACL authorization in the following situations:

- The device fails to authorize the specified ACL to the user.
- The server assigns a nonexistent ACL to the user.

This feature does not apply to VLAN authorization failure. The device logs off these users directly.

To enable the authorization-fail-offline feature:

| Step                                              | Command                                         | Remarks                                                                                                 |
|---------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                             | <b>system-view</b>                              | N/A                                                                                                     |
| 2. Enable the authorization-fail-offline feature. | <b>port-security authorization-fail offline</b> | By default, this feature is disabled, and the device does not log off users who fail ACL authorization. |

## Applying a NAS-ID profile to port security

By default, the device sends its device name in the NAS-Identifier attribute of all RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to port security globally or on a port. On a port, the device selects a NAS-ID profile in the following order:

1. The port-specific NAS-ID profile.
2. The NAS-ID profile applied globally.

If no NAS-ID profile is applied or no matching binding is found in the selected profile, the device uses the device name as the NAS-ID.

For more information about the NAS-ID profile configuration, see "[Configuring AAA](#)."

To apply a NAS-ID profile to port security:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                       | Command                                                                                                                                                                                                                                                                                                                                                           | Remarks                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 2. Apply a NAS-ID profile. | <ul style="list-style-type: none"> <li>In system view:<br/><b>port-security nas-id-profile</b> <i>profile-name</i></li> <li>In Layer 2 Ethernet interface view:<br/> <ul style="list-style-type: none"> <li>a. <b>interface</b> <i>interface-type interface-number</i></li> <li>b. <b>port-security nas-id-profile</b> <i>profile-name</i></li> </ul> </li> </ul> | By default, no NAS-ID profile is applied in system view or in interface view. |

## Displaying and maintaining port security

Execute **display** commands in any view:

| Task                                                                            | Command                                                                                                                                                       |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display the port security configuration, operation information, and statistics. | <b>display port-security</b> [ <b>interface</b> <i>interface-type interface-number</i> ]                                                                      |
| Display information about secure MAC addresses.                                 | <b>display port-security mac-address security</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>vlan</b> <i>vlan-id</i> ] [ <b>count</b> ] |
| Display information about blocked MAC addresses.                                | <b>display port-security mac-address block</b> [ <b>interface</b> <i>interface-type interface-number</i> ] [ <b>vlan</b> <i>vlan-id</i> ] [ <b>count</b> ]    |

## Port security configuration examples

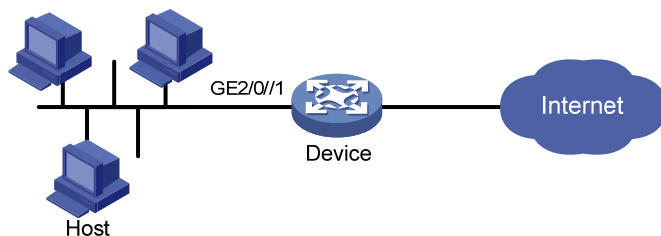
### autoLearn configuration example

#### Network requirements

As shown in [Figure 81](#), configure port GigabitEthernet 2/0/1 on the device to meet the following requirements:

- Accept a maximum of 64 users without authentication.
- Be permitted to learn and add MAC addresses as sticky MAC addresses, and set the secure MAC aging timer to 30 minutes.
- Stop learning MAC addresses after the number of secure MAC addresses reaches 64. If any frame with an unknown MAC address arrives, intrusion protection starts, and the port shuts down and stays silent for 30 seconds.

**Figure 81 Network diagram**



## Configuration procedure

```
Enable port security.
<Device> system-view
[Device] port-security enable

Set the secure MAC aging timer to 30 minutes.
[Device] port-security timer autolearn aging 30

Set port security's limit on the number of secure MAC addresses to 64 on port GigabitEthernet 2/0/1.
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] port-security max-mac-count 64

Set the port security mode to autoLearn.
[Device-GigabitEthernet2/0/1] port-security port-mode autolearn

Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.
[Device-GigabitEthernet2/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet2/0/1] quit
[Device] port-security timer disableport 30
```

## Verifying the configuration

```
Verify the port security configuration.
[Device] display port-security interface gigabitethernet 2/0/1
Port security parameters:
 Port security : Enabled
 AutoLearn aging time : 30 min
 Disableport timeout : 30 s
 MAC move : Denied
 Authorization fail : Online
 OUI value list :
```

```
GigabitEthernet2/0/1 is link-up
 Port mode : autoLearn
 NeedToKnow mode : Disabled
 Intrusion protection mode : DisablePortTemporarily
 Security MAC address attribute
 Learning mode : Sticky
 Aging type : Periodical
 Max secure MAC addresses : 64
 Current secure MAC addresses : 5
 Authorization : Permitted
```

The port allows for MAC address learning, and you can view the number of learned MAC addresses in the **Current secure MAC addresses** field.

```
Display additional information about the learned MAC addresses.
```

```
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] display this
#
interface GigabitEthernet2/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
```

```

port-security mac-address security sticky 0002-0000-0015 vlan 1
port-security mac-address security sticky 0002-0000-0014 vlan 1
port-security mac-address security sticky 0002-0000-0013 vlan 1
port-security mac-address security sticky 0002-0000-0012 vlan 1
port-security mac-address security sticky 0002-0000-0011 vlan 1
#
[Device-GigabitEthernet2/0/1] quit
Verify that the port security mode changes to secure after the number of MAC addresses learned
by the port reaches 64.
[Device] display port-security interface gigabitethernet 2/0/1
Verify that the port will be disabled for 30 seconds after it receives a frame with an unknown MAC
address. (Details not shown.)
After the port is re-enabled, delete several secure MAC addresses.
[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1
...
Verify that the port security mode of the port changes to autoLearn, and the port can learn MAC
addresses again. (Details not shown.)

```

## userLoginWithOUI configuration example

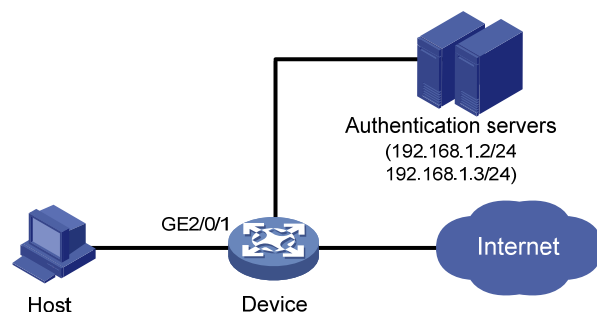
### Network requirements

As shown in [Figure 82](#), a client is connected to the device through GigabitEthernet 2/0/1. The device authenticates the client with a RADIUS server in ISP domain **sun**. If the authentication succeeds, the client is authorized to access the Internet.

- The RADIUS server at 192.168.1.2 functions as the primary authentication server and the secondary accounting server. The RADIUS server at 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is **name**, and the shared key for accounting is **money**.
- All users use the authentication, authorization, and accounting methods of ISP domain **sun**.
- The RADIUS server response timeout time is 5 seconds. The maximum number of RADIUS packet retransmission attempts is 5. The device sends real-time accounting packets to the RADIUS server at 15-minute intervals, and sends usernames without domain names to the RADIUS server.

Configure GigabitEthernet 2/0/1 to allow only one 802.1X user and a user who uses one of the specified OUI values to be authenticated.

**Figure 82 Network diagram**



## Configuration procedure

The following configuration steps cover some AAA/RADIUS configuration commands. For more information about the commands, see *Security Command Reference*.

Make sure the host and the RADIUS server can reach each other.

### 1. Configure AAA:

# Configure a RADIUS scheme named **radsun**.

```
<Device> system-view
[Device] radius scheme radsun
[Device-radius-radsun] primary authentication 192.168.1.2
[Device-radius-radsun] primary accounting 192.168.1.3
[Device-radius-radsun] secondary authentication 192.168.1.3
[Device-radius-radsun] secondary accounting 192.168.1.2
[Device-radius-radsun] key authentication simple name
[Device-radius-radsun] key accounting simple money
[Device-radius-radsun] timer response-timeout 5
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

# Configure ISP domain **sun**.

```
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

### 2. Configure 802.1X:

# Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

```
[Device] dot1x authentication-method chap
```

# Specify ISP domain **sun** as the mandatory authentication domain for 802.1X users on GigabitEthernet 2/0/1.

```
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] dot1x mandatory-domain sun
[Device-GigabitEthernet2/0/1] quit
```

### 3. Configure port security:

# Enable port security.

```
[Device] port-security enable
```

# Add five OUI values. (You can add a maximum of 16 OUI values. The port permits only one user matching one of the OUIs to pass authentication.)

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

# Set the port security mode to userLoginWithOUI.

```
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

# Verify the RADIUS scheme configuration.

[Device] display radius scheme radsun

RADIUS scheme name : radsun

Index : 0

Primary authentication server:

IP : 192.168.1.2 Port: 1812

VPN : Not configured

State: Active

Test profile: Not configured

Primary accounting server:

IP : 192.168.1.3 Port: 1813

VPN : Not configured

State: Active

Second authentication server:

IP : 192.168.1.3 Port: 1812

VPN : Not configured

State: Active

Test profile: Not configured

Second accounting server:

IP : 192.168.1.2 Port: 1813

VPN : Not configured

State: Active

Accounting-On function : Disabled

retransmission times : 50

retransmission interval(seconds) : 3

Timeout Interval(seconds) : 5

Retransmission Times : 5

Retransmission Times for Accounting Update : 5

Server Quiet Period(minutes) : 5

Realtime Accounting Interval(minutes) : 15

NAS IP Address : Not configured

VPN : Not configured

User Name Format : without-domain

Data flow unit : Megabyte

Packet unit : One

Attribute 15 check-mode : Strict

Attribute 25 : Standard

# After users pass authentication, display port security configuration. Verify that port GigabitEthernet 2/0/1 allows only one 802.1X user to be authenticated.

[Device] display port-security interface gigabitethernet 2/0/1

Port security : Enabled

AutoLearn aging time : 30 min

Disableport timeout : 30 s

MAC move : Denied

Authorization fail : Online



```

OUI value list :
 Index : 1 Value : 123401
 Index : 2 Value : 123402
 Index : 3 Value : 123403
 Index : 4 Value : 123404
 Index : 5 Value : 123405

GigabitEthernet2/0/1 is link-up
 Port mode : userLoginWithOUI
 NeedToKnow mode : Disabled
 Intrusion protection mode : NoAction
 Security MAC address attribute
 Learning mode : Sticky
 Aging type : Periodical
 Max secure MAC addresses : Not configured
 Current secure MAC addresses : 1
 Authorization : Permitted

Display information about the online 802.1X user to verify 802.1X configuration.
[Device] display dot1x

Verify that the port also allows one user whose MAC address has an OUI among the specified
OUIs to pass authentication.
[Device] display mac-address interface gigabitethernet 2/0/1

```

| MAC Address    | VLAN ID | State   | Port/NickName | Aging |
|----------------|---------|---------|---------------|-------|
| 1234-0300-0011 | 1       | Learned | GE2/0/1       | Y     |

## macAddressElseUserLoginSecure configuration example

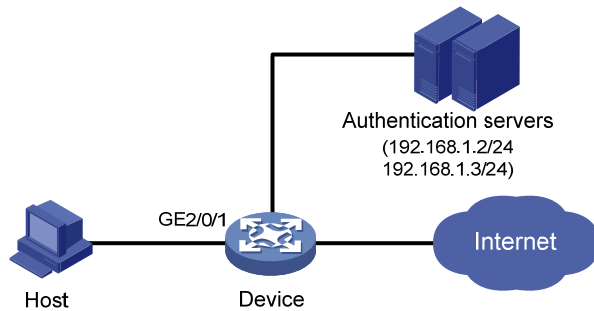
### Network requirements

As shown in [Figure 83](#), a client is connected to the device through GigabitEthernet 2/0/1. The device authenticates the client by a RADIUS server in ISP domain **sun**. If the authentication succeeds, the client is authorized to access the Internet.

Configure port GigabitEthernet 2/0/1 of the device to meet the following requirements:

- Allow more than one MAC authenticated user to log on.
- For 802.1X users, perform MAC authentication first and then, if MAC authentication fails, 802.1X authentication. Allow only one 802.1X user to log on.
- Use the MAC address of each user as the username and password for authentication. A MAC address is in the hexadecimal notation with hyphens, and letters are in upper case.
- Set the total number of MAC authenticated users and 802.1X authenticated users to 64.
- Enable NTK (**ntkonly** mode) to prevent frames from being sent to unknown MAC addresses.

Figure 83 Network diagram



## Configuration procedure

Make sure the host and the RADIUS server can reach each other.

1. Configure RADIUS authentication/accounting and ISP domain settings. (See ["userLoginWithOUI configuration example."](#))
2. Configure port security:
  - # Enable port security.
  - <Device> system-view
  - [Device] port-security enable
  - # Use MAC-based accounts for MAC authentication. Each MAC address must be in the hexadecimal notation with hyphens, and letters are in upper case.
  - [Device] mac-authentication user-name-format mac-address with-hyphen uppercase
  - # Specify the MAC authentication domain.
  - [Device] mac-authentication domain sun
  - # Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.
  - [Device] dot1x authentication-method chap
  - # Set port security's limit on the number of MAC addresses to 64 on the port.
  - [Device] interface gigabitethernet 2/0/1
  - [Device-GigabitEthernet2/0/1] port-security max-mac-count 64
  - # Set the port security mode to macAddressElseUserLoginSecure.
  - [Device-GigabitEthernet2/0/1] port-security port-mode mac-else-userlogin-secure
  - # Specify ISP domain **sun** as the mandatory authentication domain for 802.1X users.
  - [Device-GigabitEthernet2/0/1] dot1x mandatory-domain sun
  - # Set the NTK mode of the port to ntkonly.
  - [Device-GigabitEthernet2/0/1] port-security ntk-mode ntkonly
  - [Device-GigabitEthernet2/0/1] quit

## Verifying the configuration

# Verify the port security configuration.

```
[Device] display port-security interface gigabitethernet 2/0/1
```

Port security parameters:

|                      |           |
|----------------------|-----------|
| Port security        | : Enabled |
| AutoLearn aging time | : 0 min   |
| Disableport timeout  | : 30 s    |
| MAC move             | : Denied  |
| Authorization fail   | : Online  |

OUI value list

GigabitEthernet2/0/1 is link-up

Port mode : macAddressElseUserLoginSecure  
NeedToKnow mode : NeedToKnowOnly  
Intrusion protection mode : NoAction  
Security MAC address attribute  
Learning mode : Sticky  
Aging type : Periodical  
Max secure MAC addresses : 64  
Current secure MAC addresses : 0  
Authorization : Permitted

# After users pass authentication, display MAC authentication information. Verify that port GigabitEthernet 2/0/1 allows multiple MAC authentication users to be authenticated.

[Device] display mac-authentication interface gigabitethernet 2/0/1

Global MAC authentication parameters:

MAC authentication : Enabled  
User name format : MAC address in uppercase(XX-XX-XX-XX-XX-XX)  
Username : mac  
Password : Not configured  
Offline detect period : 300 s  
Quiet period : 180 s  
Server timeout : 100 s  
Authentication domain : sun  
Max MAC-auth users : 1024 per slot  
Online MAC-auth users : 3

Silent MAC users:

| MAC address | VLAN ID | From port | Port index |
|-------------|---------|-----------|------------|
|-------------|---------|-----------|------------|

GigabitEthernet2/0/1 is link-up

MAC authentication : Enabled  
Authentication domain : Not configured  
Auth-delay timer : Disabled  
Re-auth server-unreachable : Logoff  
Host mode : Single VLAN  
Max online users : 4096  
Authentication attempts : successful 3, failed 7  
Current online users : 3

| MAC address    | Auth state    |
|----------------|---------------|
| 1234-0300-0011 | Authenticated |
| 1234-0300-0012 | Authenticated |
| 1234-0300-0013 | Authenticated |

# Display 802.1X authentication information. Verify that GigabitEthernet 2/0/1 allows only one 802.1X user to be authenticated.

[Device] display dot1x interface gigabitethernet 2/0/1

Global 802.1X parameters:

802.1X authentication : Enabled

```

CHAP authentication : Enabled
Max-tx period : 30 s
Handshake period : 15 s
Quiet timer : Disabled
 Quiet period : 60 s
Supp timeout : 30 s
Server timeout : 100 s
Reauth period : 3600 s
Max auth requests : 2
SmartOn supp timeout : 30 s
SmartOn retry counts : 3
EAD assistant function : Disabled
 EAD timeout : 30 min
Domain delimiter : @
Max 802.1X users : 1024 per slot
Online 802.1X users : 1
GigabitEthernet2/0/1 is link-down
 802.1X authentication : Enabled
 Handshake : Enabled
 Handshake security : Disabled
 Unicast trigger : Disabled
 Periodic reauth : Disabled
 Port role : Authenticator
 Authorization mode : Auto
 Port access control : MAC-based
 Multicast trigger : Enabled
 Mandatory auth domain : sun
 Guest VLAN : Not configured
 Auth-Fail VLAN : Not configured
 Critical VLAN : Not configured
 Re-auth server-unreachable : Logoff
 Max online users : 4096
 SmartOn : Disabled

EAPOL packets: Tx 16331, Rx 102
Sent EAP Request/Identity packets : 16316
 EAP Request/Challenge packets: 6
 EAP Success packets: 4
 EAP Failure packets: 5
Received EAPOL Start packets : 6
 EAPOL LogOff packets: 2
 EAP Response/Identity packets : 80
 EAP Response/Challenge packets: 6
 Error packets: 0
Online 802.1X users: 1
 MAC address Auth state
 0002-0000-0011 Authenticated

```

# Verify that frames with an unknown destination MAC address, multicast address, or broadcast address are discarded. (Details not shown.)

# Troubleshooting port security

## Cannot set the port security mode

### Symptom

Cannot set the port security mode for a port.

### Analysis

For a port operating in a port security mode other than noRestrictions, you cannot change the port security mode by using the **port-security port-mode** command.

### Solution

To resolve the problem:

1. Set the port security mode to noRestrictions.  
`[Device-GigabitEthernet2/0/1] undo port-security port-mode`
2. Set a new port security mode for the port, for example, autoLearn.  
`[Device-GigabitEthernet2/0/1] port-security port-mode autolearn`
3. If the problem persists, contact Hewlett Packard Enterprise Support.

## Cannot configure secure MAC addresses

### Symptom

Cannot configure secure MAC addresses.

### Analysis

No secure MAC address can be configured on a port operating in a port security mode other than autoLearn.

### Solution

To resolve the problem:

1. Set the port security mode to autoLearn.  
`[Device-GigabitEthernet2/0/1] undo port-security port-mode`  
`[Device-GigabitEthernet2/0/1] port-security max-mac-count 64`  
`[Device-GigabitEthernet2/0/1] port-security port-mode autolearn`  
`[Device-GigabitEthernet2/0/1] port-security mac-address security 1-1-2 vlan 1`
2. If the problem persists, contact Hewlett Packard Enterprise Support.

# Configuring user profiles

## Overview

A user profile saves a set of predefined parameters, such as a CAR policy or a QoS policy.

The user profile application allows flexible traffic policing on a per-user basis. Each time a user passes authentication, the device automatically applies the parameters in the user profile to this user.

The user profile restricts authenticated user behavior as follows:

1. After the authentication server verifies a user, the server sends the device the name of the user profile specified for the user.
2. The device applies the parameters in the user profile to the user.
3. When the user logs out, the device automatically removes the user profile parameters.

## Compatibility information

### Feature and hardware compatibility

| Hardware                             | User profile compatibility |
|--------------------------------------|----------------------------|
| MSR954(JH296A/JH297A/ JH298A/JH299A) | No                         |
| MSR1002-4/1003-8S                    | Yes                        |
| MSR2003                              | Yes                        |
| MSR2004-24/2004-48                   | Yes                        |
| MSR3012/3024/3044/3064               | Yes                        |
| MSR4060/4080                         | Yes                        |

### Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## User profile configuration task list

| Tasks at a glance                                      |
|--------------------------------------------------------|
| (Required.) <a href="#">Configuring a user profile</a> |

# Configuration restrictions and guidelines

When you configure user profiles, follow these restrictions and guidelines:

- Configure authentication parameters before you create a user profile. The user profile supports working with only PPPoE authentication.
- Specify a user profile for each user account:
  - In remote authentication, specify a user profile on the authentication server.
  - In local authentication, specify a user profile in the local user view. For information about local users, see "[Configuring AAA](#)."

## Configuring a user profile

| Step                                                  | Command                                 | Remarks                                                                |
|-------------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------|
| 1. Enter system view.                                 | <b>system-view</b>                      | N/A                                                                    |
| 2. Create a user profile and enter user profile view. | <b>user-profile</b> <i>profile-name</i> | You can use the command to enter the view of an existing user profile. |

## Displaying and maintaining user profiles

Execute **display** commands in any view.

| Task                                                                                                                                                                            | Command                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Display configuration and online user information for the specified user profile or all user profiles (centralized devices in standalone mode).                                 | <b>display user-profile</b> [ <b>name</b> <i>profile-name</i> ]                                                                         |
| Display configuration and online user information for the specified user profile or all user profiles (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display user-profile</b> [ <b>name</b> <i>profile-name</i> ] [ <b>slot</b> <i>slot-number</i> ]                                      |
| Display configuration and online user information for the specified user profile or all user profiles (distributed devices in IRF mode).                                        | <b>display user-profile</b> [ <b>name</b> <i>profile-name</i> ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] |

# Configuring password control

## Overview

Password control allows you to implement the following features:

- Manage login and super password setup, expirations, and updates for device management users.
- Control user login status based on predefined policies.

Local users are divided into two types: device management users and network access users. This feature applies only to device management users. For more information about local users, see "[Configuring AAA](#)."

## Password setting

### Minimum password length

You can define the minimum length of user passwords. If a user enters a password that is shorter than the minimum length, the system rejects the password.

### Password composition policy

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters. For information about special characters, see the **password-control composition** command in *Security Command Reference*.

Depending on the system's security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters for each type, as shown in [Table 10](#).

**Table 10 Password composition policy**

| Password combination level | Minimum number of character types | Minimum number of characters for each type |
|----------------------------|-----------------------------------|--------------------------------------------|
| Level 1                    | One                               | One                                        |
| Level 2                    | Two                               | One                                        |
| Level 3                    | Three                             | One                                        |
| Level 4                    | Four                              | One                                        |

In non-FIPS mode, all the combination levels are available for a password. In FIPS mode, only the level 4 combination is available for a password.

When a user sets or changes a password, the system checks if the password meets the combination requirement. If not, the operation fails.

### Password complexity checking policy

A less complicated password such as a password containing the username or repeated characters is more likely to be cracked. For higher security, you can configure a password complexity checking policy to ensure that all user passwords are relatively complicated. With such a policy configured,



when a user configures a password, the system checks the complexity of the password. If the password is complexity-incompliant, the configuration will fail.

You can apply the following password complexity requirements:

- A password cannot contain the username or the reverse of the username. For example, if the username is abc, a password such as abc982 or 2cba is not complex enough.
- A character or number cannot be included three or more times consecutively. For example, password a111 is not complex enough.

## Password updating and expiration

### Password updating

This feature allows you to set the minimum interval at which users can change their passwords. If a user logs in to change the password but the time passed since the last change is less than this interval, the system denies the request. For example, if you set this interval to 48 hours, a user cannot change the password twice within 48 hours.

The set minimum interval is not effective when a user is prompted to change the password at the first login or after its password aging time expires.

### Password expiration

Password expiration imposes a lifecycle on a user password. After the password expires, the user needs to change the password.

If a user enters an expired password when logging in, the system displays an error message. The user is prompted to provide a new password and to confirm it by entering it again. The new password must be valid, and the user must enter exactly the same password when confirming it.

Telnet users, SSH users, and console (or AUX) users can change their own passwords. The administrator must change passwords for FTP users.

### Early notice on pending password expiration

When a user logs in, the system checks whether the password will expire in a time equal to or less than the specified notification period. If so, the system notifies the user when the password will expire and provides a choice for the user to change the password. If the user sets a new password that is complexity-compliant, the system records the new password and the setup time. If the user chooses not to change the password or the user fails to change it, the system allows the user to log in using the current password.

Telnet users, SSH users, and console (or AUX) users can change their own passwords. The administrator must change passwords for FTP users.

### Login with an expired password

You can allow a user to log in a certain number of times within a period of time after the password expires. For example, if you set the maximum number of logins with an expired password to 3 and the time period to 15 days, a user can log in three times within 15 days after the password expires.

### Password history

With this feature enabled, the system stores passwords that a user has used. When a user changes the password, the system checks the new password against the current password and those stored in the password history records. The new password must be different from the current one and those stored in the history records by at least four characters. The four characters must be different from one another. Otherwise, the system will display an error message, and the password will not be changed.

You can set the maximum number of history password records for the system to maintain for each user. When the number of history password records exceeds your setting, the most recent record overwrites the earliest one.

Current login passwords of device management users are not stored in the password history, because a device management user password is saved in cipher text and cannot be recovered to a plaintext password.

## User login control

### First login

With the global password control feature enabled, users must change the password at first login before they can access the system. In this situation, password changes are not subject to the minimum change interval.

### Login attempt limit

Limiting the number of consecutive login failures can effectively prevent password guessing.

Login attempt limit takes effect on FTP and VTY users. It does not take effect on the following types of users:

- Nonexistent users (users not configured on the device).
- Users logging in to the device through console or AUX ports.

If a user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. After making the maximum number of consecutive attempts, login attempt limit limits the user and user account in any of the following ways:

- Disables the user account until the account is manually removed from the password control blacklist.
- Allows the user to continue using the user account. The user's IP address and user account are removed from the password control blacklist when the user uses this account to successfully log in to the device.
- Disables the user account for a period of time.

The user can use the account to log in when either of the following conditions exists:

- The locking timer expires.
- The account is manually removed from the password control blacklist before the locking timer expires.

---

#### NOTE:

This account is locked only for this user. Other users can still use this account, and the blacklisted user can use other user accounts.

---

### Maximum account idle time

You can set the maximum account idle time for user accounts. When an account is idle for this period of time since the last successful login, the account becomes invalid.

## Password not displayed in any form

For security purposes, nothing is displayed when a user enters a password.

## Logging

The system logs all successful password changing events and user adding events to the password control blacklist.

# FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "[Configuring FIPS](#)") and non-FIPS mode.

## Password control configuration task list

The password control features can be configured in several different views, and different views support different features. The settings configured in different views or for different objects have the following application ranges:

- Settings for super passwords apply only to super passwords.
- Settings in local user view apply only to the password of the local user.
- Settings in user group view apply to the passwords of the local users in the user group if you do not configure password policies for these users in local user view.
- Global settings in system view apply to the passwords of the local users in all user groups if you do not configure password policies for these users in both local user view and user group view.

For local user passwords, the settings with a smaller application scope have higher priority.

To configure password control, perform the following tasks:

| Tasks at a glance                                                          |
|----------------------------------------------------------------------------|
| (Required.) <a href="#">Enabling password control</a>                      |
| (Optional.) <a href="#">Setting global password control parameters</a>     |
| (Optional.) <a href="#">Setting user group password control parameters</a> |
| (Optional.) <a href="#">Setting local user password control parameters</a> |
| (Optional.) <a href="#">Setting super password control parameters</a>      |

## Enabling password control

To successfully enable the global password control feature and allow device management users to log in to the device, the device must have sufficient storage space.

Enabling the global password control feature is the prerequisite for all password control configurations to take effect. Then, for a specific password control feature to take effect, enable this password control feature.

After the global password control feature is enabled, you cannot display the password and super password configurations for device management users by using the corresponding **display** commands. However, the configuration for network access user passwords can be displayed. The first password configured for device management users must contain at least four different characters.

To enable password control:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                                       | Command                                                                   | Remarks                                                                                                                                                                                                                                   |
|------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Enable the global password control feature.             | <b>password-control enable</b>                                            | <ul style="list-style-type: none"> <li>In non-FIPS mode, the global password control feature is disabled by default.</li> <li>In FIPS mode, the global password control feature is enabled, and cannot be disabled by default.</li> </ul> |
| 3. (Optional.) Enable a specific password control feature. | <b>password-control { aging   composition   history   length } enable</b> | By default, all four password control features are enabled.                                                                                                                                                                               |

## Setting global password control parameters

The password expiration time, minimum password length, and password composition policy can be configured in system view, user group view, or local user view. The password settings with a smaller application scope have higher priority. Global settings in system view apply to the passwords of the local users in all user groups if you do not configure password policies for these users in both local user view and user group view.

The **password-control login-attempt** command takes effect immediately and can affect the users already in the password control blacklist. Other password control configurations do not take effect on users that have been logged in or passwords that have been configured.

To set global password control parameters:

| Step                                                                 | Command                                                                                                     | Remarks                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                          | N/A                                                                                                                                                                                                                                                                                                      |
| 2. Set the password expiration time.                                 | <b>password-control aging</b><br><i>aging-time</i>                                                          | The default setting is 90 days.                                                                                                                                                                                                                                                                          |
| 3. Set the minimum password update interval.                         | <b>password-control update</b><br><i>interval interval</i>                                                  | The default setting is 24 hours.                                                                                                                                                                                                                                                                         |
| 4. Set the minimum password length.                                  | <b>password-control length</b> <i>length</i>                                                                | <ul style="list-style-type: none"> <li>In non-FIPS mode, the default setting is 10 characters.</li> <li>In FIPS mode, the default length is 15 characters.</li> </ul>                                                                                                                                    |
| 5. Configure the password composition policy.                        | <b>password-control composition</b><br><i>type-number type-number</i><br>[ <i>type-length type-length</i> ] | <ul style="list-style-type: none"> <li>In non-FIPS mode, a default password must contain at least one character type and at least one character for each type.</li> <li>In FIPS mode, a default password must contain at least four character types and at least one character for each type.</li> </ul> |
| 6. Configure the password complexity checking policy.                | <b>password-control complexity</b><br>{ <i>same-character</i>   <i>user-name</i> }<br><b>check</b>          | By default, the system does not perform password complexity checking.                                                                                                                                                                                                                                    |
| 7. Set the maximum number of history password records for each user. | <b>password-control history</b><br><i>max-record-num</i>                                                    | The default setting is 4.                                                                                                                                                                                                                                                                                |

| Step                                                                                                              | Command                                                                                                                                      | Remarks                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. Configure the login attempt limit.                                                                             | <b>password-control login-attempt</b><br><i>login-times</i> [ <b>exceed</b> { <b>lock</b>   <b>lock-time</b> <i>time</i>   <b>unlock</b> } ] | By default, the maximum number of login attempts is 3 and a user failing to log in after the specified number of attempts must wait for 1 minute before trying again. |
| 9. Set the number of days during which a user is notified of the pending password expiration.                     | <b>password-control alert-before-expire</b> <i>alert-time</i>                                                                                | The default setting is 7 days.                                                                                                                                        |
| 10. Set the maximum number of days and maximum number of times that a user can log in after the password expires. | <b>password-control expired-user-login delay</b> <i>delay times times</i>                                                                    | By default, a user can log in three times within 30 days after the password expires.                                                                                  |
| 11. Set the maximum account idle time.                                                                            | <b>password-control login idle-time</b> <i>idle-time</i>                                                                                     | The default setting is 90 days.                                                                                                                                       |

## Setting user group password control parameters

| Step                                                                     | Command                                                                                                                                      | Remarks                                                                                                                          |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                    | <b>system-view</b>                                                                                                                           | N/A                                                                                                                              |
| 2. Create a user group and enter user group view.                        | <b>user-group</b> <i>group-name</i>                                                                                                          | By default, no user group exists.<br>For information about how to configure a user group, see <a href="#">"Configuring AAA."</a> |
| 3. Configure the password expiration time for the user group.            | <b>password-control aging</b><br><i>aging-time</i>                                                                                           | By default, the password expiration time of the user group equals the global password expiration time.                           |
| 4. Configure the minimum password length for the user group.             | <b>password-control length</b> <i>length</i>                                                                                                 | By default, the minimum password length of the user group equals the global minimum password length.                             |
| 5. Configure the password composition policy for the user group.         | <b>password-control composition</b><br><i>type-number type-number</i><br>[ <b>type-length</b> <i>type-length</i> ]                           | By default, the password composition policy of the user group equals the global password composition policy.                     |
| 6. Configure the password complexity checking policy for the user group. | <b>password-control complexity</b><br>{ <b>same-character</b>   <b>user-name</b> }<br><b>check</b>                                           | By default, the password complexity checking policy of the user group equals the global password complexity checking policy.     |
| 7. Configure the login attempt limit.                                    | <b>password-control login-attempt</b><br><i>login-times</i> [ <b>exceed</b> { <b>lock</b>   <b>lock-time</b> <i>time</i>   <b>unlock</b> } ] | By default, the login-attempt policy of the user group equals the global login-attempt policy.                                   |

# Setting local user password control parameters

| Step                                                                     | Command                                                                                                                                      | Remarks                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                    | <b>system-view</b>                                                                                                                           | N/A                                                                                                                                                                                                                                 |
| 2. Create a device management user and enter local user view.            | <b>local-user</b> <i>user-name</i> <b>class manage</b>                                                                                       | By default, no local user exists.<br>Local user password control applies to device management users instead of network access users.<br>For information about how to configure a local user, see <a href="#">"Configuring AAA."</a> |
| 3. Configure the password expiration time for the local user.            | <b>password-control aging</b><br><i>aging-time</i>                                                                                           | By default, the setting equals that for the user group to which the local user belongs. If no expiration time is configured for the user group, the global setting applies to the local user.                                       |
| 4. Configure the minimum password length for the local user.             | <b>password-control length</b> <i>length</i>                                                                                                 | By default, the setting equals that for the user group to which the local user belongs. If no minimum password length is configured for the user group, the global setting applies to the local user.                               |
| 5. Configure the password composition policy for the local user.         | <b>password-control composition</b><br><i>type-number type-number</i><br>[ <b>type-length</b> <i>type-length</i> ]                           | By default, the settings equal those for the user group to which the local user belongs. If no password composition policy is configured for the user group, the global settings apply to the local user.                           |
| 6. Configure the password complexity checking policy for the local user. | <b>password-control complexity</b><br>{ <b>same-character</b>   <b>user-name</b> }<br><b>check</b>                                           | By default, the settings equal those for the user group to which the local user belongs. If no password complexity checking policy is configured for the user group, the global settings apply to the local user.                   |
| 7. Configure the login attempt limit.                                    | <b>password-control login-attempt</b><br><i>login-times</i> [ <b>exceed</b> { <b>lock</b>   <b>lock-time</b> <i>time</i>   <b>unlock</b> } ] | By default, the settings equal those for the user group to which the local user belongs. If no login-attempt policy is configured for the user group, the global settings apply to the local user.                                  |

## Setting super password control parameters

The super password allows you to obtain a temporary user role without reconnecting to the device. For more information, see *Fundamentals Configuration Guide*.

To set super password control parameters:

| Step                                                              | Command                                                                                                 | Remarks                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                             | <b>system-view</b>                                                                                      | N/A                                                                                                                                                                                                                                                                                                                  |
| 2. Set the password expiration time for super passwords.          | <b>password-control super aging</b><br><i>aging-time</i>                                                | The default setting is 90 days.                                                                                                                                                                                                                                                                                      |
| 3. Configure the minimum length for super passwords.              | <b>password-control super length</b><br><i>length</i>                                                   | <ul style="list-style-type: none"> <li>In non-FIPS mode, the default setting is 10 characters.</li> <li>In FIPS mode, the default setting is 15 characters.</li> </ul>                                                                                                                                               |
| 4. Configure the password composition policy for super passwords. | <b>password-control super composition type-number</b><br><i>type-number [ type-length type-length ]</i> | <ul style="list-style-type: none"> <li>In non-FIPS mode, a default super password must contain at least one character type and at least one character for each type.</li> <li>In FIPS mode, a default super password must contain at least four character types and at least one character for each type.</li> </ul> |

## Displaying and maintaining password control

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                               | Command                                                                                                                                      |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Display password control configuration.                            | <b>display password-control</b> [ <b>super</b> ]                                                                                             |
| Display information about users in the password control blacklist. | <b>display password-control blacklist</b> [ <b>user-name</b> <i>name</i>   <b>ip</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> ] |
| Delete users from the password control blacklist.                  | <b>reset password-control blacklist</b> [ <b>user-name</b> <i>name</i> ]                                                                     |
| Clear history password records.                                    | <b>reset password-control history-record</b> [ <b>user-name</b> <i>name</i>   <b>super</b> [ <b>role</b> <i>role name</i> ] ]                |

### NOTE:

The **reset password-control history-record** command can delete the history password records of one or all users even when the password history feature is disabled.

## Password control configuration example

### Network requirements

Configure a global password control policy to meet the following requirements:

- A password must contain at least 16 characters.
- A password must contain at least four character types and at least four characters for each type.
- An FTP or VTY user failing to provide the correct password in two successive login attempts is permanently prohibited from logging in.
- A user can log in five times within 60 days after the password expires.

- A password expires after 30 days.
- The minimum password update interval is 36 hours.
- The maximum account idle time is 30 days.
- A password cannot contain the username or the reverse of the username.
- No character appears consecutively three or more times in a password.

Configure a super password control policy for user role **network-operator** to meet the following requirements:

- A super password must contain at least 24 characters.
- A super password must contain at least four character types and at least five characters for each type.

Configure a password control policy for the local Telnet user **test** to meet the following requirements:

- The password must contain at least 24 characters.
- The password must contain at least four character types and at least five characters for each type.
- The password for the local user expires after 20 days.

## Configuration procedure

# Enable the password control feature globally.

```
<Sysname> system-view
```

```
[Sysname] password-control enable
```

# Disable a user account permanently if a user fails two consecutive login attempts on the user account.

```
[Sysname] password-control login-attempt 2 exceed lock
```

# Set all passwords to expire after 30 days.

```
[Sysname] password-control aging 30
```

# Globally set the minimum password length to 16 characters.

```
[Sysname] password-control length 16
```

# Set the minimum password update interval to 36 hours.

```
[Sysname] password-control update-interval 36
```

# Specify that a user can log in five times within 60 days after the password expires.

```
[Sysname] password-control expired-user-login delay 60 times 5
```

# Set the maximum account idle time to 30 days.

```
[Sysname] password-control login idle-time 30
```

# Refuse any password that contains the username or the reverse of the username.

```
[Sysname] password-control complexity user-name check
```

# Specify that no character can be included three or more times consecutively in a password.

```
[Sysname] password-control complexity same-character check
```

# Globally specify that all passwords must each contain at least four character types and at least four characters for each type.

```
[Sysname] password-control composition type-number 4 type-length 4
```

# Set the minimum super password length to 24 characters.

```
[Sysname] password-control super length 24
```

# Specify that a super password must contain at least four character types and at least five characters for each type.



```

[Sysname] password-control super composition type-number 4 type-length 5
Configure a super password used for switching to user role network-operator as
123456789ABGFTweuix@#$$! in plain text.
[Sysname] super password network-operator simple 123456789ABGFTweuix@#$$!
Create a device management user named test.
[Sysname] local-user test class manage
Set the service type of the user to Telnet.
[Sysname-luser-manage-test] service-type telnet
Set the minimum password length to 24 for the local user.
[Sysname-luser-manage-test] password-control length 24
Specify that the password of the local user must contain at least four character types and at least
five characters for each type.
[Sysname-luser-manage-test] password-control composition type-number 4 type-length 5
Set the password for the local user to expire after 20 days.
[Sysname-luser-manage-test] password-control aging 20
Configure the password of the local user in interactive mode.
[Sysname-luser-manage-test] password
Password:
Confirm :
Updating user information. Please wait
[Sysname-luser-manage-test] quit

```

## Verifying the configuration

```

Display the global password control configuration.
<Sysname> display password-control
Global password control configurations:
Password control: Enabled
Password aging: Enabled (30 days)
Password length: Enabled (16 characters)
Password composition: Enabled (4 types, 4 characters per type)
Password history: Enabled (max history record:4)
Early notice on password expiration: 7 days
Maximum login attempts: 2
Action for exceeding login attempts: Lock
Minimum interval between two updates: 36 hours
User account idle time: 30 days
Logins with aged password: 5 times in 60 days
Password complexity: Enabled (username checking)
 Enabled (repeated characters checking)

Display the password control configuration for super passwords.
<Sysname> display password-control super
Super password control configurations:
Password aging: Enabled (90 days)
Password length: Enabled (24 characters)
Password composition: Enabled (4 types, 5 characters per type)

Display the password control configuration for local user test.

```

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.
```

Device management user test:

State: Active

Service type: Telnet

User group: system

Bind attributes:

Authorization attributes:

Work directory: flash:

User role list: network-operator

Password control configurations:

Password aging: Enabled (20 days)

Password length: Enabled (24 characters)

Password composition: Enabled (4 types, 5 characters per type)

# Managing public keys

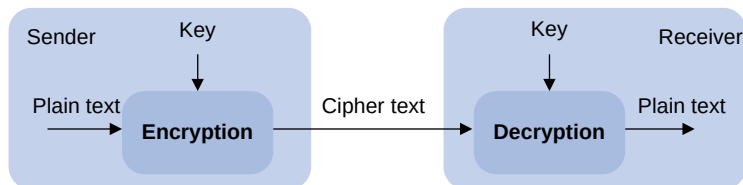
## Overview

This chapter describes public key management for the following asymmetric key algorithms:

- Revest-Shamir-Adleman Algorithm (RSA).
- Digital Signature Algorithm (DSA).
- Elliptic Curve Digital Signature Algorithm (ECDSA).

Many security applications, including SSH, SSL, and PKI, use asymmetric key algorithms to secure communications between two parties, as shown in [Figure 84](#). Asymmetric key algorithms use two separate keys (one public and one private) for encryption and decryption. Symmetric key algorithms use only one key.

**Figure 84 Encryption and decryption**



A key owner can distribute the public key in plain text on the network but must keep the private key in privacy. It is mathematically infeasible to calculate the private key even if an attacker knows the algorithm and the public key.

The security applications use the asymmetric key algorithms for the following purposes:

- **Encryption and decryption**—Any public key receiver can use the public key to encrypt information, but only the private key owner can decrypt the information.
- **Digital signature**—The key owner uses the private key to digitally sign information to be sent. The receiver decrypts the information with the sender's public key to verify information authenticity.

RSA, DSA, and ECDSA can all perform digital signature, but only RSA can perform encryption and decryption.

Asymmetric key algorithms enable secure key distribution on an insecure network. The security strength of an asymmetric key varies by the key modulus length as with any symmetric key algorithm.

## FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see ["Configuring FIPS"](#)) and non-FIPS mode.

## Creating a local key pair

When you create a local key pair, follow these guidelines:

- The key algorithm must be the same as required by the security application.

- Enter an appropriate key modulus length at the prompt (see [Table 11](#)). The longer the key modulus length, the higher the security, the longer the key generation time.
- If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The key pair name must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.
- The key pairs are automatically saved and can survive system reboots.

**Table 11 A comparison of different types of asymmetric key algorithms**

| Type  | Number of key pairs                                                                                                                                                                                                                                                                                                                                                                                                               | Modulus length                                                                                                                                                                                       |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RSA   | <ul style="list-style-type: none"> <li>• In non-FIPS mode: <ul style="list-style-type: none"> <li>◦ One host key pair, if you specify a key pair name.</li> <li>◦ One server key pair and one host key pair, if you do not specify a key pair name. Both key pairs use their default names.</li> </ul> </li> <li>• In FIPS mode: One host key pair.</li> </ul> <p><b>NOTE:</b><br/>Only SSH 1.5 uses the RSA server key pair.</p> | <ul style="list-style-type: none"> <li>• In non-FIPS mode: 512 to 2048 bits and defaults to 1024 bits. To ensure security, use a minimum of 768 bits.</li> <li>• In FIPS mode: 2048 bits.</li> </ul> |
| DSA   | One host key pair.                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• In non-FIPS mode: 512 to 2048 bits and defaults to 1024 bits. To ensure security, use a minimum of 768 bits.</li> <li>• In FIPS mode: 2048 bits.</li> </ul> |
| ECDSA | One host key pair.                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• In non-FIPS mode: 192 bits, 256 bits, 384 bits, or 521 bits.</li> <li>• In FIPS mode: 256 bits, 384 bits, or 521 bits.</li> </ul>                           |

To create a local key pair:

| Step                        | Command                                                                                                                                                                                                                                                                                                                                      | Remarks                               |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 1. Enter system view.       | <b>system-view</b>                                                                                                                                                                                                                                                                                                                           | N/A                                   |
| 2. Create a local key pair. | <ul style="list-style-type: none"> <li>• In non-FIPS mode:<br/><b>public-key local create { dsa   ecdsa [ secp192r1   secp256r1   secp384r1   secp521r1 ]   rsa } [ name key-name ]</b></li> <li>• In FIPS mode:<br/><b>public-key local create { dsa   ecdsa { secp256r1   secp384r1   secp521r1 }   rsa } [ name key-name ]</b></li> </ul> | By default, no local key pairs exist. |

## Distributing a local host public key

You must distribute a local host public key to a peer device so the peer device can perform the following operations:

- Use the public key to encrypt information sent to the local device.

- Authenticate the digital signature signed by the local device.

To distribute a local host public key, you must first export or display the key.

- Export a host public key:
  - Export a host public to a file.
  - Export a host public key to the monitor screen, and then save it to a file.

After the key is exported to a file, transfer the file to the peer device. On the peer device, import the key from the file.

- Display a host public key.  
After the key is displayed, record the key, for example, copy it to an unformatted file. On the peer device, you must literally enter the key.

## Exporting a host public key

When you export a host public key, follow these restrictions and guidelines:

- If you specify a file name in the command, the command exports the key to the specified file.
- If you do not specify a file name, the command exports the key to the monitor screen. You must manually save the exported key to a file.

To export a local host public key:

| Step                               | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.              | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2. Export a local host public key. | <ul style="list-style-type: none"> <li>• Export an RSA host public key:               <ul style="list-style-type: none"> <li>◦ In non-FIPS mode:<br/><b>public-key local export rsa [ name key-name ] { openssh   ssh1   ssh2 } [ filename ]</b></li> <li>◦ In FIPS mode:<br/><b>public-key local export rsa [ name key-name ] { openssh   ssh2 } [ filename ]</b></li> </ul> </li> <li>• Export a DSA host public key:<br/><b>public-key local export dsa [ name key-name ] { openssh   ssh2 } [ filename ]</b></li> </ul> |

## Displaying a host public key

Perform the following tasks in any view:

| Task                           | Command                                                      |
|--------------------------------|--------------------------------------------------------------|
| Display local RSA public keys. | <b>display public-key local rsa public [ name key-name ]</b> |
| Display local DSA public keys. | <b>display public-key local dsa public [ name key-name ]</b> |

### NOTE:

Do not distribute the RSA server public key **serverkey (default)** to a peer device.

## Destroying a local key pair

To avoid key compromise, destroy the local key pair and generate a new pair after any of the following conditions occurs:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The local certificate has expired. For more information about local certificates, see "[Configuring PKI](#)."

To destroy a local key pair:

| Step                         | Command                                                                     |
|------------------------------|-----------------------------------------------------------------------------|
| 1. Enter system view.        | <b>system-view</b>                                                          |
| 2. Destroy a local key pair. | <b>public-key local destroy { dsa   ecdsa   rsa }<br/>[ name key-name ]</b> |

## Configuring a peer host public key

To encrypt information sent to a peer device or authenticate the digital signature of the peer device, you must configure the peer device's public key on the local device.

You can configure the peer host public key by using the following methods:

- Import the peer host public key from a public key file (recommended).
- Manually enter (type or copy) the peer host public key.

### Importing a peer host public key from a public key file

Before you perform this task, make sure you have exported the host public key to a file on the peer device and obtained the file from the peer device. For information about exporting a host public key, see "[Exporting a host public key](#)."

After you import the key, the system automatically converts the imported public key to a string in the Public Key Cryptography Standards (PKCS) format.

To import a peer host public key from a public key file:

| Step                                                     | Command                                                   | Remarks                                     |
|----------------------------------------------------------|-----------------------------------------------------------|---------------------------------------------|
| 1. Enter system view.                                    | <b>system-view</b>                                        | N/A                                         |
| 2. Import a peer host public key from a public key file. | <b>public-key peer keyname import<br/>sshkey filename</b> | By default, no peer host public keys exist. |

### Entering a peer host public key

Before you perform this task, make sure you have displayed the key on the peer device and recorded the key. For information about displaying a host public key, see "[Displaying a host public key](#)."

Use the **display public-key local public** command to display the public key on the peer device. The format of the public key displayed in any other way might be incorrect. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, the system saves the key.

To enter a peer host public key:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                                                      | Command                               | Remarks                                                                                 |
|---------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------------------------------------------------|
| 2. Specify a name for the peer host public key and enter public key view. | <b>public-key peer</b> <i>keyname</i> | By default, no peer host public keys exist.                                             |
| 3. Type or copy the key.                                                  | N/A                                   | You can use spaces and carriage returns, but the system does not save them.             |
| 4. Return to system view.                                                 | <b>peer-public-key end</b>            | When you exit public key view, the system automatically saves the peer host public key. |

## Displaying and maintaining public keys

Execute **display** commands in any view.

| Task                           | Command                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Display local public keys.     | <b>display public-key local</b> { <i>dsa</i>   <i>ecdsa</i>   <i>rsa</i> } <b>public</b> [ <i>name key-name</i> ] |
| Display peer host public keys. | <b>display public-key peer</b> [ <i>brief</i>   <i>name publickey-name</i> ]                                      |

## Examples of public key management

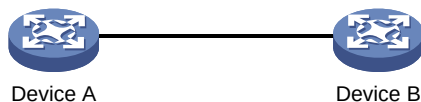
### Example for entering a peer host public key

#### Network requirements

As shown in [Figure 85](#), to prevent illegal access, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.

- Configure Device B to use the asymmetric key algorithm of RSA to authenticate Device A.
- Manually specify the host public key of Device A on Device B.

**Figure 85 Network diagram**



#### Configuration procedure

1. Configure Device A:  
 # Create local RSA key pairs with default names on Device A, and use the default modulus length 1024 bits.  

```

<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:

```

```

Generating Keys...
.....+++++
.....+++++
.....+++++
.....+++++
Create the key pair successfully.
Display all local RSA public keys.
[DeviceA] display public-key local rsa public
=====
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
45FDDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
CB47440AF6BB25ACA50203010001
=====
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
AC41C80A15953FB22AA30203010001

```

## 2. Configure Device B:

# Enter the host public key of Device A in public key view. The key must be literally the same as displayed on Device A.

```
<DeviceB> system-view
```

```
[DeviceB] public-key peer devicea
```

Enter public key view. Return to system view with "peer-public-key end" command.

```
[DeviceB-pkey-public-key-devicea]30819F300D06092A864886F70D010101050003818D003081890
```

```
2818100DA3B90F59237347B
```

```
[DeviceB-pkey-public-key-devicea]8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027A
```

```
C8F04A827B30C2CAF79242E
```

```
[DeviceB-pkey-public-key-devicea]45FDDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D2
```

```
88EC54A5D31EFAE4F681257
```

```
[DeviceB-pkey-public-key-devicea]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94E
```

```
B1F2D561BF66EA27DFD4788
```

```
[DeviceB-pkey-public-key-devicea]CB47440AF6BB25ACA50203010001
```

# Save the public key and return to system view.

```
[DeviceB-pkey-public-key-devicea] peer-public-key end
```



## Verifying the configuration

# Verify that the peer host public key configured on Device B is the same as the key displayed on Device A.

```
[DeviceB] display public-key peer name devicea
```

```
=====
```

```
Key name: devicea
```

```
Key type: RSA
```

```
Key modulus: 1024
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
```

```
8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
```

```
45FDDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
```

```
6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
```

```
CB47440AF6BB25ACA50203010001
```

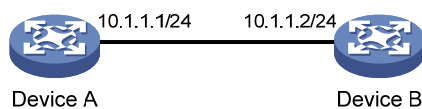
## Example for importing a public key from a public key file

### Network requirements

As shown in [Figure 86](#), Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.

- Configure Device B to use the asymmetric key algorithm of RSA to authenticate Device A.
- Import the host public key of Device A from the public key file to Device B.

**Figure 86 Network diagram**



### Configuration procedure

#### 1. Configure Device A:

# Create local RSA key pairs with default names on Device A, and use the default modulus length 1024 bits.

```
<DeviceA> system-view
```

```
[DeviceA] public-key local create rsa
```

The range of public key modulus is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

```
.....++++++
```

```
.....++++++
```

```
....++++++
```

```
.....++++++
```

Create the key pair successfully.

# Display all local RSA public keys.

```
[DeviceA] display public-key local rsa public
```

```

=====
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
 30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
 8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
 45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
 6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
 CB47440AF6BB25ACA50203010001
=====

```

```

Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
 307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
 1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
 E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
 AC41C80A15953FB22AA30203010001

```

# Export the RSA host public key to the file **devicea.pub**.

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
```

```
[DeviceA] quit
```

# Enable the FTP server function, create an FTP user with the username **ftp** and password **123**, and configure the FTP user role as **network-admin**.

```
[DeviceA] ftp server enable
```

```
[DeviceA] local-user ftp
```

```
[DeviceA-luser-manage-ftp] password simple 123
```

```
[DeviceA-luser-manage-ftp] service-type ftp
```

```
[DeviceA-luser-manage-ftp] authorization-attribute user-role network-admin
```

```
[DeviceA-luser-manage-ftp] quit
```

## 2. Configure Device B:

# Use FTP in binary mode to get the public key file **devicea.pub** from Device A.

```
<DeviceB> ftp 10.1.1.1
```

```
Connected to 10.1.1.1 (10.1.1.1).
```

```
220 FTP service ready.
```

```
User(10.1.1.1:(none)):ftp
```

```
331 Password required for ftp.
```

```
Password:
```

```
230 User logged in.
```

```
Remote system type is UNIX.
```

```
Using binary mode to transfer files.
```

```
ftp> binary
```

```
200 TYPE is now 8-bit binary
```

```
ftp> get devicea.pub
```

```
227 Entering Passive Mode (10,1,1,1,118,252)
```

```
150 Accepted data connection
```

```
226 File successfully transferred
```

```
301 bytes received in 0.003 seconds (98.0 kbyte/s)
```

```

ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
Import the host public key from the key file devicea.pub.
<DeviceB> system-view
[DeviceB] public-key peer devicea import sshkey devicea.pub

```

## Verifying the configuration

# Verify that the peer host public key configured on Device B is the same as the key displayed on Device A.

```
[DeviceB] display public-key peer name devicea
```

```
=====
```

```
Key name: devicea
```

```
Key type: RSA
```

```
Key modulus: 1024
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
```

```
8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
```

```
45FDF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
```

```
6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
```

```
CB47440AF6BB25ACA50203010001
```

# Configuring PKI

## Overview

Public Key Infrastructure (PKI) is an asymmetric key infrastructure to encrypt and decrypt data for securing network services. Data encrypted with the public key can be decrypted only with the private key. Likewise, data encrypted with the private key can be decrypted only with the public key.

PKI uses digital certificates to distribute and employ public keys, and provides network communication and e-commerce with security services such as user authentication, data confidentiality, and data integrity.

Hewlett Packard Enterprise's PKI system provides certificate management for IPsec and SSL.

## PKI terminology

### Digital certificate

A digital certificate is an electronic document signed by a CA that binds a public key with the identity of its owner.

A digital certificate includes the following information:

- Issuer name (name of the CA that issued the certificate).
- Subject name (name of the individual or group to which the certificate is issued).
- Identity information of the subject.
- Subject's public key.
- Signature of the CA.
- Validity period.

A digital certificate must comply with the international standards of ITU-T X.509, of which X.509 v3 is the most commonly used.

This chapter covers the following types of certificates:

- **CA certificate**—Certificate of a CA. Multiple CAs in a PKI system form a CA tree, with the root CA at the top. The root CA generates a self-signed certificate, and each lower level CA holds a CA certificate issued by the CA immediately above it. The chain of these certificates forms a chain of trust.
- **Registration authority (RA) certificate**—Certificate issued by a CA to an RA. RAs act as proxies for CAs to process enrollment requests in a PKI system.
- **Local certificate**—Digital certificate issued by a CA to a local PKI entity, which contains the entity's public key.
- **Peer certificate**—CA-signed digital certificate of a peer, which contains the peer's public key.

### Certificate revocation list

A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked. A CRL is created and signed by the CA that originally issued the certificates.

The CA publishes CRLs periodically to revoke certificates. Entities that are associated with the revoked certificates should not be trusted.

The CA must revoke a certificate when any of the following conditions occurs:

- The certificate subject name is changed.
- The private key is compromised.

- The association between the subject and CA is changed. For example, when an employee terminates employment with an organization.

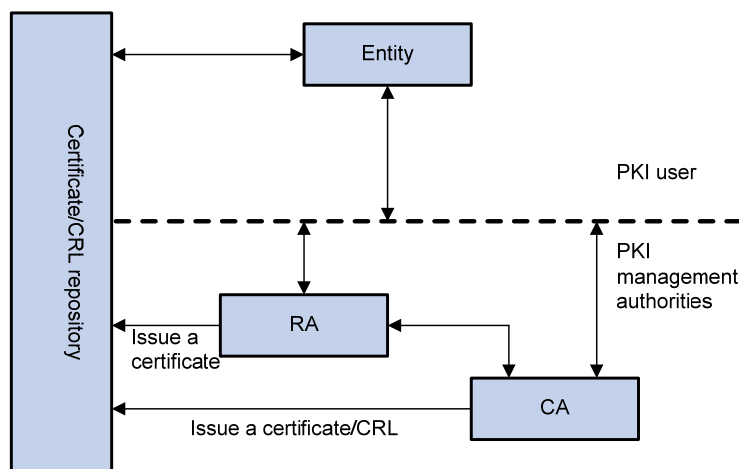
## CA policy

A CA policy is a set of criteria that a CA follows to process certificate requests, to issue and revoke certificates, and to publish CRLs. Typically, a CA advertises its policy in a certification practice statement (CPS). You can obtain a CA policy through out-of-band means such as phone, disk, and email. Make sure you understand the CA policy before you select a trusted CA for certificate request because different CAs might use different policies.

## PKI architecture

A PKI system consists of PKI entities, CAs, RAs and a certificate/CRL repository, as shown in [Figure 87](#).

**Figure 87 PKI architecture**



- **PKI entity**—An end user using PKI certificates. The PKI entity can be an operator, an organization, a device like a router or a switch, or a process running on a computer. PKI entities use SCEP to communicate with the CA or RA.
- **CA**—Certification authority that grants and manages certificates. A CA issues certificates, defines the certificate validity periods, and revokes certificates by publishing CRLs.
- **RA**—Registration authority, which offloads the CA by processing enrollment requests. The RA accepts certificate requests, verifies user identity, and determines whether to ask the CA to issue certificates.

The RA is optional in a PKI system. In cases when the CA operates over a wide geographical area or when there is security concern over exposing the CA to direct network access, it is advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates and CRLs.

- **Certificate/CRL repository**—A certificate distribution point that stores certificates and CRLs, and distributes these certificates and CRLs to PKI entities. It also provides the query function. A PKI repository can be a directory server using the LDAP or HTTP protocol, of which LDAP is commonly used.

## PKI operation

The following workflow describes how a PKI entity requests a local certificate from a CA that has RAs:

1. A PKI entity submits a certificate request to the RA.

2. The RA verifies the identity of the entity and sends a digital signature containing the identity information and the public key to the CA.
3. The CA verifies the digital signature, approves the request, and issues a certificate.
4. After receiving the certificate from the CA, the RA sends the certificate to the certificate repositories and notifies the PKI entity that the certificate has been issued.
5. The entity obtains the certificate from the certificate repository.

## PKI applications

The PKI technology can meet security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

- **VPN**—A VPN is a private data communication network built on the public communication infrastructure. A VPN can use network layer security protocols (for example, IPsec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.
- **Secure emails**—PKI can address the email requirements for confidentiality, integrity, authentication, and non-repudiation. A common secure email protocol is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.
- **Web security**—PKI can be used in the SSL handshake phase to verify the identities of the communicating parties by digital certificates.

## Support for MPLS L3VPN

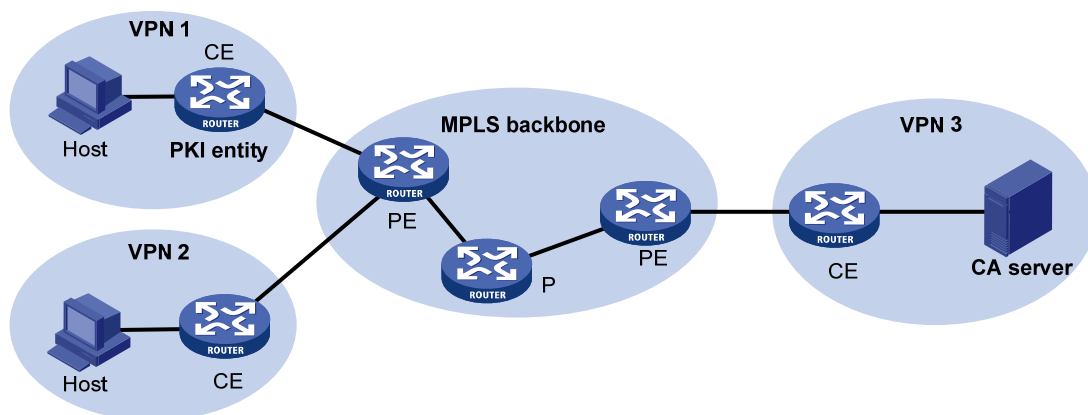
An enterprise might have multiple branches in different VPNs. PKI support for MPLS L3VPN is required if users in different VPNs request certificates from the CA server in the headquarters VPN.

As shown in [Figure 88](#), the PKI entity in VPN 1 requests a certificate from the CA server in VPN 3 in the following workflow:

1. The PKI entity submits a certificate request to the CA server.
2. The PE device that connects to the PKI entity transmits the request to the CA server through MPLS L3VPN.
3. The CA server verifies the request and issues the certificate.
4. The PE device that connects to the CA server transmits the certificate to the PKI entity.

For information about MPLS L3VPN, see *MPLS Configuration Guide*.

**Figure 88 PKI support for MPLS L3VPN**



# FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "[Configuring FIPS](#)") and non-FIPS mode.

## PKI configuration task list

| Tasks at a glance                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Required.) <a href="#">Configuring a PKI entity</a>                                                                                                                                                                           |
| (Required.) <a href="#">Configuring a PKI domain</a>                                                                                                                                                                           |
| (Required.) <a href="#">Requesting a certificate</a> : <ul style="list-style-type: none"><li>• <a href="#">Configuring automatic certificate request</a></li><li>• <a href="#">Manually requesting a certificate</a></li></ul> |
| (Optional.) <a href="#">Aborting a certificate request</a>                                                                                                                                                                     |
| (Optional.) <a href="#">Obtaining certificates</a>                                                                                                                                                                             |
| (Optional.) <a href="#">Verifying PKI certificates</a>                                                                                                                                                                         |
| (Optional.) <a href="#">Specifying the storage path for the certificates and CRLs</a>                                                                                                                                          |
| (Optional.) <a href="#">Exporting certificates</a>                                                                                                                                                                             |
| (Optional.) <a href="#">Removing a certificate</a>                                                                                                                                                                             |
| (Optional.) <a href="#">Configuring a certificate-based access control policy</a>                                                                                                                                              |

## Configuring a PKI entity

A certificate applicant uses an entity to provide its identity information to a CA. A valid PKI entity must include one or more of following identity categories:

- Distinguished name (DN) of the entity, which further includes the common name, county code, locality, organization, unit in the organization, and state. If you configure the DN for an entity, a common name is required.
- FQDN of the entity.
- IP address of the entity.

Whether the categories are required or optional depends on the CA policy. Follow the CA policy to configure the entity settings. For example, if the CA policy requires the entity DN, but you configure only the IP address, the CA rejects the certificate request from the entity.

The SCEP add-on on the Windows 2000 CA server has restrictions on the data length of a certificate request. If a request from a PKI entity exceeds the data length limit, the CA server does not respond to the certificate request. In this case, you can use an out-of-band means to submit the request. Other types of CA servers, such as RSA servers and OpenCA servers, do not have such restrictions.

To configure a PKI entity:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                               | Command                                                                                          | Remarks                                                                                  |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 2. Create a PKI entity and enter its view.         | <b>pki entity</b> <i>entity-name</i>                                                             | By default, no PKI entities exist.<br>To create multiple PKI entities, repeat this step. |
| 3. Set a common name for the entity.               | <b>common-name</b> <i>common-name-string</i>                                                     | By default, the common name is not set.                                                  |
| 4. Set the country code of the entity.             | <b>country</b> <i>country-code-string</i>                                                        | By default, the country code is not set.                                                 |
| 5. Set the locality of the entity.                 | <b>locality</b> <i>locality-name</i>                                                             | By default, the locality is not set.                                                     |
| 6. Set the organization of the entity.             | <b>organization</b> <i>org-name</i>                                                              | By default, the organization is not set.                                                 |
| 7. Set the unit of the entity in the organization. | <b>organization-unit</b> <i>org-unit-name</i>                                                    | By default, the unit is not set.                                                         |
| 8. Set the state where the entity resides.         | <b>state</b> <i>state-name</i>                                                                   | By default, the state is not set.                                                        |
| 9. Set the FQDN of the entity.                     | <b>fqdn</b> <i>fqdn-name-string</i>                                                              | By default, the FQDN is not set.                                                         |
| 10. Configure the IP address of the entity.        | <b>ip</b> { <i>ip-address</i>   <b>interface</b> <i>interface-type</i> <i>interface-number</i> } | By default, the IP address is not configured.                                            |

## Configuring a PKI domain

A PKI domain contains enrollment information for a PKI entity. It is locally significant and is intended only for reference by other applications like IKE and SSL.

To configure a PKI domain:

| Step                                                            | Command                                                                                           | Remarks                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                           | <b>system-view</b>                                                                                | N/A                                                                                                                                                                                                                                                                                                       |
| 2. Create a PKI domain and enter its view.                      | <b>pki domain</b> <i>domain-name</i>                                                              | By default, no PKI domains exist.                                                                                                                                                                                                                                                                         |
| 3. Specify the trusted CA.                                      | <b>ca identifier</b> <i>name</i>                                                                  | By default, no trusted CA is specified.<br>To obtain a CA certificate, the trusted CA name must be provided. The trusted CA name uniquely identifies the CA to be used if multiple CAs exist on the same CA server. The CA server's URL is specified by using the <b>certificate request url</b> command. |
| 4. Specify the PKI entity name.                                 | <b>certificate request entity</b> <i>entity-name</i>                                              | By default, no entity is specified.                                                                                                                                                                                                                                                                       |
| 5. Specify the type of certificate request reception authority. | <b>certificate request from</b> { <i>ca</i>   <i>ra</i> }                                         | By default, no authority type is specified.                                                                                                                                                                                                                                                               |
| 6. Specify the certificate request URL.                         | <b>certificate request url</b> <i>url-string</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] | By default, the certificate request URL is not specified.                                                                                                                                                                                                                                                 |



| Step                                                                                     | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. (Optional.) Set the SCEP polling interval and maximum number of polling attempts.     | <b>certificate request polling</b> { <b>count</b> <i>count</i>   <b>interval</b> <i>minutes</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | By default, the device polls the CA server for the certificate request status every 20 minutes. The maximum number of polling attempts is 50.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 8. (Optional.) Specify the LDAP server.                                                  | <b>ldap-server host</b> <i>hostname</i> [ <b>port</b> <i>port-number</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | This task is required only when the CRL repository is an LDAP server and the URL of the CRL repository does not contain the host name of the LDAP server.<br><br>By default, no LDAP server is specified.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 9. Enter a fingerprint to be matched against the fingerprint of the root CA certificate. | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/><b>root-certificate fingerprint</b> { <b>md5</b>   <b>sha1</b> } <i>string</i></li> <li>In FIPS mode:<br/><b>root-certificate fingerprint sha1</b> <i>string</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>Before a PKI entity can enroll with a CA, it must authenticate the CA by obtaining the self-signed certificate of the CA and verifying the fingerprint of the CA certificate.</p> <p>If a fingerprint is not entered in the PKI domain, and if the CA certificate is imported or obtained through manual certificate request, you must verify the fingerprint that is displayed during authentication of the CA certificate.</p> <p>If the CA certificate is obtained through automatic certificate request, the certificate will be rejected if a fingerprint has not been entered.</p> <p>By default, no fingerprint is specified.</p> |
| 10. Specify the key pair for certificate request.                                        | <ul style="list-style-type: none"> <li>Specify an RSA key pair:<br/><b>public-key rsa</b> { { <b>encryption name</b> <i>encryption-key-name</i> [ <b>length</b> <i>key-length</i> ]   <b>signature name</b> <i>signature-key-name</i> [ <b>length</b> <i>key-length</i> ] } *   <b>general name</b> <i>key-name</i> [ <b>length</b> <i>key-length</i> ] }</li> <li>Specify an ECDSA key pair:<br/><b>public-key ecdsa name</b> <i>key-name</i> [ <b>secp192r1</b>   <b>secp256r1</b>   <b>secp384r1</b>   <b>secp521r1</b> ]</li> <li>Specify a DSA key pair:<br/><b>public-key dsa name</b> <i>key-name</i> [ <b>length</b> <i>key-length</i> ]</li> </ul> | <p>By default, no key pair is specified.</p> <p>If the specified key pair does not exist, the PKI entity automatically creates the key pair before submitting a certificate request.</p> <p>For information about how to generate DSA, ECDSA, and RSA key pairs, see "<a href="#">Managing public keys</a>."</p>                                                                                                                                                                                                                                                                                                                            |
| 11. (Optional.) Specify the intended use for the certificate.                            | <b>usage</b> { <b>ike</b>   <b>ssl-client</b>   <b>ssl-server</b> } *                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>By default, the certificate can be used by all applications, including IKE, SSL clients, and SSL server.</p> <p>The extension options contained in an issued certificate depend on the CA policy, and they might be different from those specified in the PKI domain.</p>                                                                                                                                                                                                                                                                                                                                                                |

| Step                                                                      | Command                                                                                                                                                                                                                                                                                                                                                                                                                    | Remarks                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12. (Optional.) Specify a source IP address for the PKI protocol packets. | <ul style="list-style-type: none"> <li>Specify the source IPv4 address for the PKI protocol packets:<br/><b>source ip</b> { <i>ip-address</i>   <b>interface</b> { <i>interface-type</i> <i>interface-number</i> } }</li> <li>Specify the source IPv6 address for the PKI protocol packets:<br/><b>source ipv6</b> { <i>ipv6-address</i>   <b>interface</b> { <i>interface-type</i> <i>interface-number</i> } }</li> </ul> | <p>This task is required if the CA policy requires that the CA server accept certificate requests from a specific IP address or subnet.</p> <p>By default, the source IP address of PKI protocol packets is the IP address of their outgoing interface.</p> |

## Requesting a certificate

To request a certificate, a PKI entity must provide its identity information and public key to a CA.

A certificate request can be submitted to a CA in offline or online mode.

- **Offline mode**—A certificate request is submitted by using an out-of-band method, such as phone, disk, or email. You can use this mode as required or if you fail to request a certificate in online mode.

To submit a certificate request in offline mode:

- Use **pki request-certificate domain pkcs10** to print the request information on the terminal or use **pki request-certificate domain pkcs10 filename** to save the request information to a local file.
  - Send the printed information or the saved file to the CA by using an out-of-band method.
- **Online mode**—A certificate request can be automatically or manually submitted. This section describes the online request mode.

## Configuration guidelines

The following guidelines apply to certificate request for an entity in a PKI domain:

- Make sure the device is time synchronized with the CA server. Otherwise, the certificate request might fail because the certificate might be considered to be outside of the validity period. For information about how to configure the system time, see *Fundamentals Configuration Guide*.
- To request a new certificate for a PKI entity that already has a local certificate, perform the following tasks:
  - Use the **pki delete-certificate** command to delete the existing local certificate.
  - Use the **public-key local create** to generate a new key pair. The new key pair will automatically overwrite the old key pair in the domain.
  - Submit a new certificate request.
- After a new certificate is obtained, do not use the **public-key local create** or **public-key local destroy** command to generate or destroy a key pair with the same name as the key pair in the local certificate. Otherwise, the existing local certificate becomes unavailable.
- A PKI domain can have local certificates using only one type of cryptographic algorithms (DSA, ECDSA, or RSA). If DSA or ECDSA is used, a PKI domain can have only one local certificate. If RSA is used, a PKI domain can have one local certificate for signature, and one local certificate for encryption.

# Configuring automatic certificate request

## ❗ IMPORTANT:

The device does not support automatic certificate rollover. To avoid service interruptions, you must manually submit a certificate renewal request before the current certificate expires.

In auto request mode, a PKI entity with no local certificates automatically submits a certificate request to the CA when an application works with the PKI entity. For example, when IKE negotiation uses a digital signature for identity authentication, but no local certificate is available, the entity automatically submits a certificate request. It saves the certificate locally after obtaining the certificate from the CA.

A CA certificate must be present before you request a local certificate. If no CA certificate exists in the PKI domain, the PKI entity automatically obtains a CA certificate before sending a certificate request.

To configure automatic certificate request:

| Step                                         | Command                                                                                                    | Remarks                                                                                                                                       |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                        | <b>system-view</b>                                                                                         | N/A                                                                                                                                           |
| 2. Enter PKI domain view.                    | <b>pki domain</b> <i>domain-name</i>                                                                       | N/A                                                                                                                                           |
| 3. Set the certificate request mode to auto. | <b>certificate request mode auto</b> [ <b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i> ] | By default, the manual request mode applies.<br>In auto request mode, set a password for certificate revocation as required by the CA policy. |

## Manually requesting a certificate

Before you manually submit a certificate request, make sure the CA certificate exists and a key pair is specified for the PKI domain:

- The CA certificate is used to verify the authenticity and validity of the obtained local certificate.
- The key pair is used for certificate request. Upon receiving the public key and the identity information, the CA signs and issues a certificate.

After the CA issues the certificate, the device obtains and saves it locally.

To manually request a certificate:

| Step                                           | Command                                         | Remarks                                      |
|------------------------------------------------|-------------------------------------------------|----------------------------------------------|
| 1. Enter system view.                          | <b>system-view</b>                              | N/A                                          |
| 2. Enter PKI domain view.                      | <b>pki domain</b> <i>domain-name</i>            | N/A                                          |
| 3. Set the certificate request mode to manual. | <b>certificate request mode manual</b>          | By default, the manual request mode applies. |
| 4. Return to system view.                      | <b>quit</b>                                     | N/A                                          |
| 5. Obtain a CA certificate.                    | See " <a href="#">Obtaining certificates.</a> " | N/A                                          |

| Step                                                                                 | Command                                                                                                                                                  | Remarks                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6. Submit a certificate request or generate a certificate request in PKCS#10 format. | <b>pki request-certificate domain</b><br><i>domain-name</i> [ <b>password</b> <i>password</i> ]<br>[ <b>pkcs10</b> [ <i>filename</i> <i>filename</i> ] ] | This command is not saved in the configuration file.<br><br>This command triggers the PKI entity to automatically generate a key pair if the key pair specified in the PKI domain does not exist. The name, algorithm, and length of the key pair are configured in the PKI domain. |

## Aborting a certificate request

Before the CA issues a certificate, you can abort a certificate request and change its parameters, such as the common name, country code, or FQDN. You can use the **display pki certificate request-status** command to display the status of a certificate request.

Alternatively, you also can remove a PKI domain to abort the associated certificate request.

To abort a certificate request:

| Step                            | Command                                                        | Remarks                                              |
|---------------------------------|----------------------------------------------------------------|------------------------------------------------------|
| 1. Enter system view.           | <b>system-view</b>                                             | N/A                                                  |
| 2. Abort a certificate request. | <b>pki abort-certificate-request domain</b> <i>domain-name</i> | This command is not saved in the configuration file. |

## Obtaining certificates

You can obtain the CA certificate, local certificates, and peer certificates related to a PKI domain from a CA and save them locally for higher lookup efficiency. To do so, use either the offline mode or the online mode:

- In offline mode, obtain the certificates by an out-of-band means like FTP, disk, or email, and then import them locally. Use this mode when the CRL repository is not specified, the CA server does not support SCEP, or the CA server generates the key pair for the certificates.
- In online mode, you can obtain the CA certificate through SCEP and obtain local certificates or peer certificates through LDAP.

## Configuration prerequisites

To obtain local or peer certificates in online mode, specify the LDAP server for the PKI domain.

To import local or peer certificates in offline mode, perform the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, display and copy the contents of a certificate to a file on the device. Make sure the certificate is in PEM format because only certificates in PEM format can be imported.
- To import a certificate, a CA certificate chain must exist in the PKI domain, or be contained in the certificate. If the CA certificate chain is not available, obtain it before importing the certificate.

## Configuration guidelines

- To import a local certificate containing an encrypted key pair, you must provide the challenge password. Contact the CA administrator to obtain the password.
- If a CA certificate already exists locally, you cannot obtain it again in online mode. If you want to obtain a new one, use the **pki delete-certificate** command to remove the existing CA certificate and local certificates first.
- If local or peer certificates already exist, you can obtain new local or peer certificates to overwrite the existing ones. If RSA is used, a PKI domain can have two local certificates, one for signature and the other for encryption.
- If CRL checking is enabled, obtaining a certificate triggers CRL checking. If the certificate to be obtained has been revoked, the certificate cannot be obtained.
- The device compares the validity period of a certificate with the local system time to determine whether the certificate is valid. Make sure the system time of the device is synchronized with the CA server.

## Configuration procedure

To obtain certificates:

| Step                    | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Remarks                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 1. Enter system view.   | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | N/A                                                                                 |
| 2. Obtain certificates. | <ul style="list-style-type: none"><li>• Import certificates in offline mode:<br/><b>pki import domain</b> <i>domain-name</i> { <b>der</b> { <b>ca</b>   <b>local</b>   <b>peer</b> } <b>filename</b> <i>filename</i>   <b>p12</b> <b>local</b> <i>filename filename</i>   <b>pem</b> { <b>ca</b>   <b>local</b>   <b>peer</b> } [ <b>filename</b> <i>filename</i> ] }</li><li>• Obtain certificates in online mode:<br/><b>pki retrieve-certificate domain</b> <i>domain-name</i> { <b>ca</b>   <b>local</b>   <b>peer</b> <i>entity-name</i> }</li></ul> | The <b>pki retrieve-certificate</b> command is not saved in the configuration file. |

## Verifying PKI certificates

A certificate is automatically verified when it is requested, obtained, or used by an application. If the certificate expires, if it is not issued by a trusted CA, or if it is revoked, the certificate cannot be used.

You can also manually verify a certificate. If it has been revoked, the certificate cannot be requested or obtained.

## Verifying certificates with CRL checking

CRL checking checks whether a certificate is in the CRL. If it is, the certificate has been revoked and its home entity is not trusted.

To use CRL checking, a CRL must be obtained from a CRL repository. The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

If no CRL repository is found after the selection process, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

When verifying the CA certificate of a PKI domain, the system needs to verify all the certificates in the CA certificate chain of the domain. To ensure a successful certificate verification process, the device must contain all the PKI domains to which the CA certificates in the certificate chain belong.

Each CA certificate contains an issuer field that identifies the parent CA that issued the certificate. After identifying the parent certificate of a certificate, the system locates the PKI domains to which the parent certificate belongs. If CRL checking is enabled for the domains, the system checks whether or not the CA certificate has been revoked. The process continues until the root CA certificate is reached. The system verifies that each CA certificate in the certificate chain is issued by the named parent CA, starting from the root CA.

To verify certificates with CRL checking:

| Step                                                  | Command                                                                                | Remarks                                                                                                                                                          |
|-------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                 | <b>system-view</b>                                                                     | N/A                                                                                                                                                              |
| 2. Enter PKI domain view.                             | <b>pki domain</b> <i>domain-name</i>                                                   | N/A                                                                                                                                                              |
| 3. (Optional.) Specify the URL of the CRL repository. | <b>crl url</b> <i>url-string</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]      | By default, the URL of the CRL repository is not specified.                                                                                                      |
| 4. Enable CRL checking.                               | <b>crl check enable</b>                                                                | By default, CRL checking is enabled.                                                                                                                             |
| 5. Return to system view.                             | <b>quit</b>                                                                            | N/A                                                                                                                                                              |
| 6. Obtain the CA certificate.                         | See " <a href="#">Obtaining certificates.</a> "                                        | N/A                                                                                                                                                              |
| 7. (Optional.) Obtain the CRL and save it locally.    | <b>pki retrieve-crl domain</b> <i>domain-name</i>                                      | The newly obtained CRL overwrites the old one, if any.<br>The obtained CRL must be issued by a CA certificate in the CA certificate chain in the current domain. |
| 8. Manually verify the validity of the certificates.  | <b>pki validate-certificate domain</b> <i>domain-name</i> { <b>ca</b>   <b>local</b> } | N/A                                                                                                                                                              |

## Verifying certificates without CRL checking

| Step                                                 | Command                                                                                | Remarks                                              |
|------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------|
| 1. Enter system view.                                | <b>system-view</b>                                                                     | N/A                                                  |
| 2. Enter PKI domain view.                            | <b>pki domain</b> <i>domain-name</i>                                                   | N/A                                                  |
| 3. Disable CRL checking.                             | <b>undo crl check enable</b>                                                           | By default, CRL checking is enabled.                 |
| 4. Return to system view.                            | <b>quit</b>                                                                            | N/A                                                  |
| 5. Obtain the CA certificate.                        | See " <a href="#">Obtaining certificates.</a> "                                        | N/A                                                  |
| 6. Manually verify the validity of the certificates. | <b>pki validate-certificate domain</b> <i>domain-name</i> { <b>ca</b>   <b>local</b> } | This command is not saved in the configuration file. |

# Specifying the storage path for the certificates and CRLs

## ⚠ CAUTION:

If you change the storage path, save the configuration before you reboot or shut down the device to avoid loss of the certificates or the CRLs.

The device has a default storage path for certificates and CRLs. You can change the storage path and specify different paths for the certificates and CRLs.

After you change the storage path for certificates or CRLs, the certificate files (with the .cer or .p12 extension) and CRL files (with the .crl extension) in the original path are moved to the new path.

To specify the storage path for certificates and CRLs:

| Task                                                | Command                                             | Remarks                                                                                                                                                                                                        |
|-----------------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specify the storage path for certificates and CRLs. | <b>pki storage { certificates   crls } dir-path</b> | By default, the device stores certificates and CRLs in the PKI directory on the storage media of the device.<br><br>For a distributed device, the specified directory must be on the active MPU of the device. |

# Exporting certificates

## ❗ IMPORTANT:

To export all certificates in the PKCS12 format, the PKI domain must have a minimum of one local certificate. Otherwise, the certificates in the PKI domain cannot be exported.

You can export the CA certificate and the local certificates in a PKI domain to certificate files. The exported certificate files can then be imported back to the device or other PKI applications.

When you export a local certificate with the RSA key pair, the name of the target file might be different than the file name specified with the **filename** keyword. It depends on the purpose of the key pair of the certificate.

To export certificates:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                    | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Remarks                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 2. Export certificates. | <ul style="list-style-type: none"> <li>Export certificates in DER format:<br/><b>pki export domain</b> <i>domain-name</i> <b>der</b> { <b>all</b>   <b>ca</b>   <b>local</b> } <b>filename</b> <i>filename</i></li> <li>Export certificates in PKCS12 format:<br/><b>pki export domain</b> <i>domain-name</i> <b>p12</b> { <b>all</b>   <b>local</b> } <b>passphrase</b> <i>p12passwordstring</i> <b>filename</b> <i>filename</i></li> <li>Export certificates in PEM format:<br/><b>pki export domain</b> <i>domain-name</i> <b>pem</b> { { <b>all</b>   <b>local</b> } [ { <b>3des-cbc</b>   <b>aes-128-cbc</b>   <b>aes-192-cbc</b>   <b>aes-256-cbc</b>   <b>des-cbc</b> } <i>pempasswordstring</i> ]   <b>ca</b> } [ <b>filename</b> <i>filename</i> ]</li> </ul> | If you do not specify a file name when you export a certificate in PEM format, the certificate is displayed on the terminal. |

## Removing a certificate

You can remove the CA certificate, local certificate, or peer certificates in a PKI domain. After you remove the CA certificate, the system automatically removes the local certificates, peer certificates, and CRLs in the domain.

You can remove a local certificate and request a new one when the local certificate is about to expire or the certificate's private key is compromised. To remove a local certificate and request a new certificate, perform the following tasks:

1. Remove the local certificate.
2. Use the **public-key local destroy** command to destroy the existing local key pair.
3. Use the **public-key local create** command to generate a new key pair.
4. Request a new certificate.

To remove a certificate:

| Step                     | Command                                                                                                                                | Remarks                                                                                                            |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.    | <b>system-view</b>                                                                                                                     | N/A                                                                                                                |
| 2. Remove a certificate. | <b>pki delete-certificate domain</b> <i>domain-name</i> { <b>ca</b>   <b>local</b>   <b>peer</b> [ <b>serial</b> <i>serial-num</i> ] } | If you use the <b>peer</b> keyword without specifying a serial number, this command removes all peer certificates. |

## Configuring a certificate-based access control policy

Certificate-based access control policies allow you to authorize access to a device (for example, an HTTPS server) based on the attributes of an authenticated client's certificate.

A certificate-based access control policy is a set of access control rules (permit or deny statements), each associated with a certificate attribute group. A certificate attribute group contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field.

If a certificate matches all attribute rules in a certificate attribute group associated with an access control rule, the system determines that the certificate matches the access control rule. In this



scenario, the match process stops, and the system performs the access control action defined in the access control rule.

The following conditions describe how a certificate-based access control policy verifies the validity of a certificate:

- If a certificate matches a permit statement, the certificate passes the verification.
- If a certificate matches a deny statement or does not match any statements in the policy, the certificate is regarded invalid.
- If a statement is associated with a non-existing attribute group, or the attribute group does not have attribute rules, the certificate matches the statement.
- If the certificate-based access control policy referenced by a security application (for example, HTTPS) does not exist, all certificates in the application pass the verification.

To configure a certificate-based access control policy:

| Step                                                                                                   | Command                                                                                                                                                                                                                                                        | Remarks                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                                                  | <b>system-view</b>                                                                                                                                                                                                                                             | N/A                                                                                                                                                                                                                            |
| 2. Create a certificate attribute group and enter its view.                                            | <b>pki certificate attribute-group</b><br><i>group-name</i>                                                                                                                                                                                                    | By default, no certificate attribute groups exist.                                                                                                                                                                             |
| 3. (Optional.) Configure an attribute rule for issuer name, subject name, or alternative subject name. | <b>attribute</b> <i>id</i> { <b>alt-subject-name</b> { <b>fqdn</b>   <b>ip</b> }   { <b>issuer-name</b>   <b>subject-name</b> } { <b>dn</b>   <b>fqdn</b>   <b>ip</b> } }<br>{ <b>ctn</b>   <b>equ</b>   <b>nctn</b>   <b>nequ</b> }<br><i>attribute-value</i> | By default, not attribute rules are configured.                                                                                                                                                                                |
| 4. Return to system view.                                                                              | <b>quit</b>                                                                                                                                                                                                                                                    | N/A                                                                                                                                                                                                                            |
| 5. Create a certificate-based access control policy and enter its view.                                | <b>pki certificate access-control-policy</b><br><i>policy-name</i>                                                                                                                                                                                             | By default, no certificate-based access control policy exists.                                                                                                                                                                 |
| 6. Create a certificate access control rule.                                                           | <b>rule</b> [ <i>id</i> ] { <b>deny</b>   <b>permit</b> }<br><i>group-name</i>                                                                                                                                                                                 | By default, no certificate access control rules are configured, and all certificates can pass the verification.<br><br>You can create multiple certificate access control rules for a certificate-based access control policy. |

## Displaying and maintaining PKI

Execute **display** commands in any view.

| Task                                                         | Command                                                                                                                                 |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Display the contents of a certificate.                       | <b>display pki certificate domain</b> <i>domain-name</i> { <b>ca</b>   <b>local</b>   <b>peer</b> [ <b>serial</b> <i>serial-num</i> ] } |
| Display certificate request status.                          | <b>display pki certificate request-status</b> [ <b>domain</b> <i>domain-name</i> ]                                                      |
| Display locally stored CRLs in a PKI domain.                 | <b>display pki crl domain</b> <i>domain-name</i>                                                                                        |
| Display certificate attribute group information.             | <b>display pki certificate attribute-group</b> [ <i>group-name</i> ]                                                                    |
| Display certificate-based access control policy information. | <b>display pki certificate access-control-policy</b> [ <i>policy-name</i> ]                                                             |

# PKI configuration examples

You can use different software applications, such as Windows server, RSA Keon, and OpenCA, to act as the CA server.

If you use Windows server or OpenCA, you must install the SCEP add-on for Windows server or enable SCEP for OpenCA. In either case, when you configure a PKI domain, you must use the **certificate request from ra** command to specify the RA to accept certificate requests.

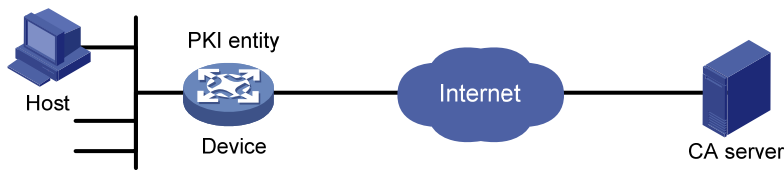
If you use RSA Keon, the SCEP add-on is not required. When you configure a PKI domain, you must use the **certificate request from ca** command to specify the CA to accept certificate requests.

## Requesting a certificate from an RSA Keon CA server

### Network requirements

Configure the PKI entity (the device) to request a local certificate from the CA server.

Figure 89 Network diagram



### Configuring the RSA Keon CA server

1. Create a CA server named **myca**:

In this example, you must configure these basic attributes on the CA server:

- **Nickname**—Name of the trusted CA.
- **Subject DN**—DN attributes of the CA, including the common name (CN), organization unit (OU), organization (O), and country (C).

You can use the default values for other attributes.

2. Configure extended attributes:

Configure parameters in the **Jurisdiction Configuration** section on the management page of the CA server:

- Select the correct extension profiles.
- Enable the SCEP autovetting function to enable the CA server to automatically approve certificate requests without manual intervention.
- Specify the IP address list for SCEP autovetting.

### Configuring the device

1. Synchronize the system time of the device with the CA server for the device to correctly request certificates or obtain CRLs. (Details not shown.)

2. Create an entity named **aaa** and set the common name to **Device**.

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name Device
[Device-pki-entity-aaa] quit
```

3. Configure a PKI domain:

```
Create a PKI domain named torsa and enter its view.
[Device] pki domain torsa
```

# Specify the name of the trusted CA. The setting must be the same as CA name configured on the CA server. This example uses **myca**.

```
[Device-pki-domain-torsa] ca identifier myca
```

# Configure the URL of the CA server. The URL format is **http://host:port/Issuing Jurisdiction ID**, where *Issuing Jurisdiction ID* is a hexadecimal string generated on the CA server.

```
[Device-pki-domain-torsa] certificate request url
http://1.1.2.22:446/80f6214aa8865301d07929ae481c7ceed99f95bd
```

# Configure the device to send certificate requests to **ca**.

```
[Device-pki-domain-torsa] certificate request from ca
```

# Set the PKI entity name to **aaa**.

```
[Device-pki-domain-torsa] certificate request entity aaa
```

# Specify the URL of the CRL repository.

```
[Device-pki-domain-torsa] crl url ldap://1.1.2.22:389/CN=myca
```

# Configure a general-purpose RSA key pair named **abc** with a length of 1024 bits.

```
[Device-pki-domain-torsa] public-key rsa general name abc length 1024
```

```
[Device-pki-domain-torsa] quit
```

**4. Generate the RSA key pair.**

```
[Device] public-key local create rsa name abc
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....++++++

.....++++++

Create the key pair successfully.

**5. Request a local certificate:**

# Obtain the CA certificate and save it locally.

```
[Device] pki retrieve-certificate domain torsa ca
```

The trusted CA's finger print is:

MD5 fingerprint: EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB

SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

Is the finger print correct?(Y/N):y

Retrieved the certificates successfully.

# Submit a certificate request manually and set the certificate revocation password to **1111**. The certificate revocation password is required when an RSA Keon CA server is used.

```
[Device] pki request-certificate domain torsa password 1111
```

Start to request the general certificate ...

.....

Request certificate of domain torsa successfully

## Verifying the configuration

# Display information about the local certificate in PKI domain **torsa**.

```
[Device] display pki certificate domain torsa local
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

15:79:75:ec:d2:33:af:5e:46:35:83:bc:bd:6e:e3:b8

```
Signature Algorithm: sha1WithRSAEncryption
Issuer: CN=myca
Validity
 Not Before: Jan 6 03:10:58 2013 GMT
 Not After : Jan 6 03:10:58 2014 GMT
Subject: CN=Device
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (1024 bit)
 Modulus:
 00:ab:45:64:a8:6c:10:70:3b:b9:46:34:8d:eb:1a:
 a1:b3:64:b2:37:27:37:9d:15:bd:1a:69:1d:22:0f:
 3a:5a:64:0c:8f:93:e5:f0:70:67:dc:cd:c1:6f:7a:
 0c:b1:57:48:55:81:35:d7:36:d5:3c:37:1f:ce:16:
 7e:f8:18:30:f6:6b:00:d6:50:48:23:5c:8c:05:30:
 6f:35:04:37:1a:95:56:96:21:95:85:53:6f:f2:5a:
 dc:f8:ec:42:4a:6d:5c:c8:43:08:bb:f1:f7:46:d5:
 f1:9c:22:be:f3:1b:37:73:44:f5:2d:2c:5e:8f:40:
 3e:36:36:0d:c8:33:90:f3:9b
 Exponent: 65537 (0x10001)
X509v3 extensions:
 X509v3 CRL Distribution Points:

 Full Name:
 DirName: CN = myca
```

```
Signature Algorithm: sha1WithRSAEncryption
b0:9d:d9:ac:a0:9b:83:99:bf:9d:0a:ca:12:99:58:60:d8:aa:
73:54:61:4b:a2:4c:09:bb:9f:f9:70:c7:f8:81:82:f5:6c:af:
25:64:a5:99:d1:f6:ec:4f:22:e8:6a:96:58:6c:c9:47:46:8c:
f1:ba:89:b8:af:fa:63:c6:c9:77:10:45:0d:8f:a6:7f:b9:e8:
25:90:4a:8e:c6:cc:b8:1a:f8:e0:bc:17:e0:6a:11:ae:e7:36:
87:c4:b0:49:83:1c:79:ce:e2:a3:4b:15:40:dd:fe:e0:35:52:
ed:6d:83:31:2c:c2:de:7c:e0:a7:92:61:bc:03:ab:40:bd:69:
1b:f5
```

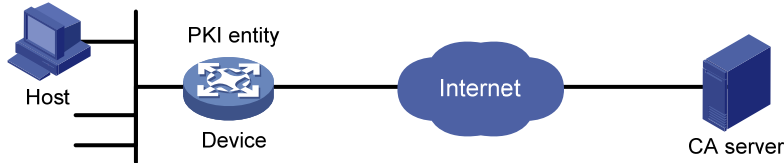
To display detailed information about the CA certificate, use the **display pki certificate domain** command.

## Requesting a certificate from a Windows Server 2003 CA server

### Network requirements

Configure the PKI entity (the device) to request a local certificate from a Windows Server 2003 CA server.

Figure 90 Network diagram



## Configuring the Windows Server 2003 CA server

1. Install the certificate service component:
  - a. Select **Control Panel > Add or Remove Programs** from the start menu.
  - b. Select **Add/Remove Windows Components > Certificate Services**.
  - c. Click **Next** to begin the installation.
  - d. Set the CA name. In this example, set the CA name to **myca**.
2. Install the SCEP add-on:

By default, Windows Server 2003 does not support SCEP. You must install the SCEP add-on on the server for a PKI entity to register and obtain a certificate from the server. After the SCEP add-on installation is complete, you will see a URL. Specify this URL as the certificate request URL on the device.
3. Modify the certificate service attributes:
  - a. Select **Control Panel > Administrative Tools > Certificate Authority** from the start menu.

If the certificate service component and SCEP add-on have been installed successfully, there should be two certificates issued by the CA to the RA.
  - b. Right-click the CA server in the navigation tree and select **Properties > Policy Module**.
  - c. Click **Properties**, and then select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.
4. Modify the Internet information services attributes:
  - a. Select **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager** from the start menu.
  - b. Select **Web Sites** from the navigation tree.
  - c. Right-click **Default Web Site** and select **Properties > Home Directory**.
  - d. Specify the path for certificate service in the **Local path** box.
  - e. Specify a unique TCP port number for the default website to avoid conflict with existing services. In this example, port 8080 is used.

## Configuring the device

1. Synchronize the device's system time with the CA server for the device to correctly request certificates. (Details not shown.)
2. Create an entity named **aaa** and set the common name to **test**.

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name test
[Device-pki-entity-aaa] quit
```
3. Configure a PKI domain:

# Create a PKI domain named **winserver** and enter its view.

```
[Device] pki domain winserver
```

# Set the name of the trusted CA to **myca**.

```
[Device-pki-domain-winserver] ca identifier myca
```

# Configure the certificate request URL. The URL format is **http://host:port/certsrv/mscep/mscep.dll**, where *host:port* is the host IP address and port number of the CA server.

```
[Device-pki-domain-winsrv] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

# Configure the device to send certificate requests to **ra**.

```
[Device-pki-domain-winsrv] certificate request from ra
```

# Set the PKI entity name to **aaa**.

```
[Device-pki-domain-winsrv] certificate request entity aaa
```

# Configure a general-purpose RSA key pair named **abc** with a length of 1024 bits.

```
[Device-pki-domain-winsrv] public-key rsa general name abc length 1024
```

```
[Device-pki-domain-winsrv] quit
```

#### 4. Generate the RSA local key pair.

```
[Device] public-key local create rsa name abc
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....+++++

.....+++++

Create the key pair successfully.

#### 5. Request a local certificate:

# Obtain the CA certificate and save it locally.

```
[Device] pki retrieve-certificate domain winsrv ca
```

The trusted CA's finger print is:

MD5 fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB

SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Retrieved the certificates successfully.

# Submit a certificate request manually.

```
[Device] pki request-certificate domain winsrv
```

Start to request the general certificate ...

...

Request certificate of domain winsrv successfully

### Verifying the configuration

# Display information about the local certificate in PKI domain **winsrv**.

```
[Device] display pki certificate domain winsrv local
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

(Negative)01:03:99:ff:ff:ff:ff:fd:11

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=sec

Validity

Not Before: Dec 24 07:09:42 2012 GMT

Not After : Dec 24 07:19:42 2013 GMT

Subject: CN=test

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c3:b5:23:a0:2d:46:0b:68:2f:71:d2:14:e1:5a:  
55:6e:c5:5e:26:86:c1:5a:d6:24:68:02:bf:29:ac:  
dc:31:41:3f:5d:5b:36:9e:53:dc:3a:bc:0d:11:fb:  
d6:7d:4f:94:3c:c1:90:4a:50:ce:db:54:e0:b3:27:  
a9:6a:8e:97:fb:20:c7:44:70:8f:f0:b9:ca:5b:94:  
f0:56:a5:2b:87:ac:80:c5:cc:04:07:65:02:39:fc:  
db:61:f7:07:c6:65:4c:e4:5c:57:30:35:b4:2e:ed:  
9c:ca:0b:c1:5e:8d:2e:91:89:2f:11:e3:1e:12:8a:  
f8:dd:f8:a7:2a:94:58:d9:c7:f8:1a:78:bd:f5:42:  
51:3b:31:5d:ac:3e:c3:af:fa:33:2c:fc:c2:ed:b9:  
ee:60:83:b3:d3:e5:8e:e5:02:cf:b0:c8:f0:3a:a4:  
b7:ac:a0:2c:4d:47:5f:39:4b:2c:87:f2:ee:ea:d0:  
c3:d0:8e:2c:80:83:6f:39:86:92:98:1f:d2:56:3b:  
d7:94:d2:22:f4:df:e3:f8:d1:b8:92:27:9c:50:57:  
f3:a1:18:8b:1c:41:ba:db:69:07:52:c1:9a:3d:b1:  
2d:78:ab:e3:97:47:e2:70:14:30:88:af:f8:8e:cb:  
68:f9:6f:07:6e:34:b6:38:6a:a2:a8:29:47:91:0e:  
25:39

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

X509v3 Subject Key Identifier:

C9:BB:D5:8B:02:1D:20:5B:40:94:15:EC:9C:16:E8:9D:6D:FD:9F:34

X509v3 Authority Key Identifier:

keyid:32:F1:40:BA:9E:F1:09:81:BD:A8:49:66:FF:F8:AB:99:4A:30:21:9

B

X509v3 CRL Distribution Points:

Full Name:

URI:file://\g07904c\CertEnroll\sec.crl

Authority Information Access:

CA Issuers - URI:http://gc/CertEnroll/gc\_sec.crt

CA Issuers - URI:file://\gc\CertEnroll\gc\_sec.crt

1.3.6.1.4.1.311.20.2:

.0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.0.f.f.l.i.n.e

Signature Algorithm: sha1WithRSAEncryption

76:f0:6c:2c:4d:bc:22:59:a7:39:88:0b:5c:50:2e:7a:5c:9d:  
6c:28:3c:c0:32:07:5a:9c:4c:b6:31:32:62:a9:45:51:d5:f5:  
36:8f:47:3d:47:ae:74:6c:54:92:f2:54:9f:1a:80:8a:3f:b2:  
14:47:fa:dc:1e:4d:03:d5:d3:f5:9d:ad:9b:8d:03:7f:be:1e:  
29:28:87:f7:ad:88:1c:8f:98:41:9a:db:59:ba:0a:eb:33:ec:  
cf:aa:9b:fc:0f:69:3a:70:f2:fa:73:ab:c1:3e:4d:12:fb:99:  
31:51:ab:c2:84:c0:2f:e5:f6:a7:c3:20:3c:9a:b0:ce:5a:bc:  
0f:d9:34:56:bc:1e:6f:ee:11:3f:7c:b2:52:f9:45:77:52:fb:  
46:8a:ca:b7:9d:02:0d:4e:c3:19:8f:81:46:4e:03:1f:58:03:  
bf:53:c6:c4:85:95:fb:32:70:e6:1b:f3:e4:10:ed:7f:93:27:  
90:6b:30:e7:81:36:bb:e2:ec:f2:dd:2b:bb:b9:03:1c:54:0a:  
00:3f:14:88:de:b8:92:63:1e:f5:b3:c2:cf:0a:d5:f4:80:47:  
6f:fa:7e:2d:e3:a7:38:46:f6:9e:c7:57:9d:7f:82:c7:46:06:  
7d:7c:39:c4:94:41:bd:9e:5c:97:86:c8:48:de:35:1e:80:14:  
02:09:ad:08

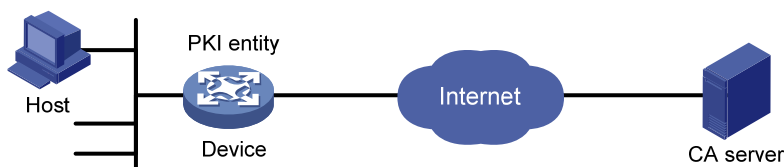
To display detailed information about the CA certificate, use the **display pki certificate domain** command.

## Requesting a certificate from an OpenCA server

### Network requirements

Configure the PKI entity (the device) to request a local certificate from the CA server.

**Figure 91 Network diagram**



### Configuring the OpenCA server

Configure the OpenCA server as instructed in related manuals. (Details not shown.)

Make sure the version of the OpenCA server is later than version 0.9.2 because the earlier versions do not support SCEP.

### Configuring the device

1. Synchronize the device's system time with the CA server for the device to correctly request certificates. (Details not shown.)
2. Create a PKI entity named **aaa** and configure the common name, country code, organization name, and OU for the entity.

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name rnd
[Device-pki-entity-aaa] country CN
```



- ```
[Device-pki-entity-aaa] organization test
[Device-pki-entity-aaa] organization-unit software
[Device-pki-entity-aaa] quit
```
3. Configure a PKI domain:


```
# Create a PKI domain named openca and enter its view.
[Device] pki domain openca

# Specify the name of the trusted CA as myca.
[Device-pki-domain-openca] ca identifier myca

# Configure the certificate request URL. The URL is in the format http://host/cgi-bin/pki/scep,
where host is the host IP address of the OpenCA server.
[Device-pki-domain-openca] certificate request url
http://192.168.222.218/cgi-bin/pki/scep

# Configure the device to send certificate requests to the RA.
[Device-pki-domain-openca] certificate request from ra

# Specify PKI entity aaa for certificate request.
[Device-pki-domain-openca] certificate request entity aaa

# Configure a general-purpose RSA key pair named abc with a length of 1024 bits.
[Device-pki-domain-openca] public-key rsa general name abc length 1024
[Device-pki-domain-openca] quit
```
 4. Generate the RSA key pair.


```
[Device] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....++++++
.....++++++
Create the key pair successfully.
```
 5. Request a local certificate:


```
# Obtain the CA certificate and save it locally.
[Device] pki retrieve-certificate domain openca ca
The trusted CA's finger print is:
      MD5  fingerprint:5AA3 DEFD 7B23 2A25 16A3 14F4 C81C C0FA
      SHA1 fingerprint:9668 4E63 D742 4B09 90E0 4C78 E213 F15F DC8E 9122
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.

# Submit a certificate request manually.
[Device] pki request-certificate domain openca
Start to request the general certificate ...
...
Request certificate of domain openca successfully
```

Verifying the configuration

- ```
Display information about the local certificate in PKI domain openca.
[Device] display pki certificate domain openca local
Certificate:
Data:
```

```

Version: 3 (0x2)
Serial Number:
 21:1d:b8:d2:e4:a9:21:28:e4:de
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CN, L=shangdi, ST=pukras, O=OpenCA Labs, OU=mysubUnit, CN=sub-ca,
DC=pki-subdomain, DC=mydomain-sub, DC=com
Validity
 Not Before: Jun 30 09:09:09 2011 GMT
 Not After : May 1 09:09:09 2012 GMT
Subject: CN=rnd, O=test, OU=software, C=CN
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (1024 bit)
 Modulus:
 00:b8:7a:9a:b8:59:eb:fc:70:3e:bf:19:54:0c:7e:
 c3:90:a5:d3:fd:ee:ff:c6:28:c6:32:fb:04:6e:9c:
 d6:5a:4f:aa:bb:50:c4:10:5c:eb:97:1d:a7:9e:7d:
 53:d5:31:ff:99:ab:b6:41:f7:6d:71:61:58:97:84:
 37:98:c7:7c:79:02:ac:a6:85:f3:21:4d:3c:8e:63:
 8d:f8:71:7d:28:a1:15:23:99:ed:f9:a1:c3:be:74:
 0d:f7:64:cf:0a:dd:39:49:d7:3f:25:35:18:f4:1c:
 59:46:2b:ec:0d:21:1d:00:05:8a:bf:ee:ac:61:03:
 6c:1f:35:b5:b4:cd:86:9f:45
 Exponent: 65537 (0x10001)
X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Cert Type:
 SSL Client, S/MIME
 X509v3 Key Usage:
 Digital Signature, Non Repudiation, Key Encipherment
 X509v3 Extended Key Usage:
 TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
Netscape Comment:
 User Certificate of OpenCA Labs
X509v3 Subject Key Identifier:
 24:71:C9:B8:AD:E1:FE:54:9A:EA:E9:14:1B:CD:D9:45:F4:B2:7A:1B
X509v3 Authority Key Identifier:
 keyid:85:EB:D5:F7:C9:97:2F:4B:7A:6D:DD:1B:4D:DD:00:EE:53:CF:FD:5B

X509v3 Issuer Alternative Name:
 DNS:root@docm.com, DNS:, IP Address:192.168.154.145, IP
Address:192.168.154.138
 Authority Information Access:
 CA Issuers - URI:http://192.168.222.218/pki/pub/cacert/cacert.crt
 OCSP - URI:http://192.168.222.218:2560/
 1.3.6.1.5.5.7.48.12 - URI:http://192.168.222.218:830/

```

X509v3 CRL Distribution Points:

Full Name:

URI:http://192.168.222.218/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption

```
5c:4c:ba:d0:a1:35:79:e6:e5:98:69:91:f6:66:2a:4f:7f:8b:
0e:80:de:79:45:b9:d9:12:5e:13:28:17:36:42:d5:ae:fc:4e:
ba:b9:61:f1:0a:76:42:e7:a6:34:43:3e:2d:02:5e:c7:32:f7:
6b:64:bb:2d:f5:10:6c:68:4d:e7:69:f7:47:25:f5:dc:97:af:
ae:33:40:44:f3:ab:e4:5a:a0:06:8f:af:22:a9:05:74:43:b6:
e4:96:a5:d4:52:32:c2:a8:53:37:58:c7:2f:75:cf:3e:8e:ed:
46:c9:5a:24:b1:f5:51:1d:0f:5a:07:e6:15:7a:02:31:05:8c:
03:72:52:7c:ff:28:37:1e:7e:14:97:80:0b:4e:b9:51:2d:50:
98:f2:e4:5a:60:be:25:06:f6:ea:7c:aa:df:7b:8d:59:79:57:
8f:d4:3e:4f:51:c1:34:e6:c1:1e:71:b5:0d:85:86:a5:ed:63:
1e:08:7f:d2:50:ac:a0:a3:9e:88:48:10:0b:4a:7d:ed:c1:03:
9f:87:97:a3:5e:7d:75:1d:ac:7b:6f:bb:43:4d:12:17:9a:76:
b0:bf:2f:6a:cc:4b:cd:3d:a1:dd:e0:dc:5a:f3:7c:fb:c3:29:
b0:12:49:5c:12:4c:51:6e:62:43:8b:73:b9:26:2a:f9:3d:a4:
81:99:31:89
```

To display detailed information about the CA certificate, use the **display pki certificate domain** command.

## Requesting a certificate from an RSA Keon CA server in an NAT-PT network

### Network requirements

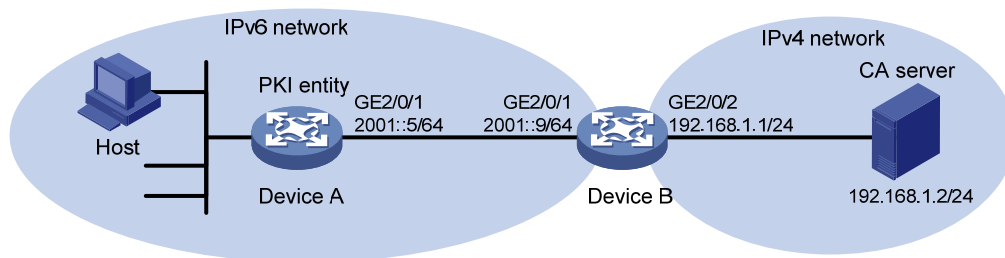
As shown in [Figure 92](#), the PKI entity (Device A) is in an IPv6 network and the CA server is in an IPv4 network.

Device A wants to connect to the CA server to obtain CRLs and to request certificates from the server.

To meet the requirements, perform the following tasks:

- Configure PKI settings on Device A.
- Deploy an NAT-PT device (Device B) between the IPv4 and IPv6 networks. Configure static mappings at the IPv4 network side and the IPv6 network side separately so that the IPv4 network and the IPv6 network can access each other.

**Figure 92 Network diagram**



## Configuring the RSA Keon CA server

1. In this example, an RSA Keon CA server acts as the CA server. For information about configuring an RSA Keon CA server, see "[Requesting a certificate from an RSA Keon CA server.](#)"
2. Enable local certificate publishing.
3. Configure a static route to the subnet 192.168.18.0/24 (the following describes the configuration on the Windows XP operating system):
  - a. Open the **cmd** window.
  - b. Enter **route add 192.16.18.0 mask 255.255.255.0 192.168.1.1**.

```
C:\Documents and Settings\username\route add 192.16.18.0 mask 255.255.255.0 192.168.1.1
```

## Configuring Device B

```
Enable IPv6.
<DeviceB> system-view
[DeviceB] ipv6

Assign an IPv6 address to interface GigabitEthernet 2/0/1, and enable NAT-PT on the interface.
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ipv6 address 2001::9/64
[DeviceB-GigabitEthernet2/0/1] natpt enable
[DeviceB-GigabitEthernet2/0/1] quit

Assign an IPv4 address to interface GigabitEthernet 2/0/2, and enable NAT-PT on the interface.
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 192.168.1.1 255.255.255.0
[DeviceB-GigabitEthernet2/0/2] natpt enable
[DeviceB-GigabitEthernet2/0/2] quit

Specify the NAT-PT prefix.
[DeviceB] natpt prefix 3001::

Configure the static mapping at the IPv4 network side.
[DeviceB] natpt v4bound static 192.168.1.2 3001::5

Configure the static mapping at the IPv6 network side.
[DeviceB] natpt v6bound static 2001::5 192.16.18.111
```

## Configuring Device A

1. Configure a static route to the subnet corresponding to the NAT-PT prefix.

```
<DeviceA> system-view
[DeviceA] ipv6 route-static 3001:: 16 2001::9
```
2. Create an entity named **aaa** and set its common name to **test**.

```
[DeviceA] pki entity aaa
[DeviceA-pki-entity-aaa] common-name test
[DeviceA-pki-entity-aaa] quit
```
3. Configure a PKI domain:
  - # Create a PKI domain named **torsa** and enter its view.

```
[DeviceA] pki domain torsa
```
  - # Specify the name of the trusted CA as **myca**.

```
[DeviceA-pki-domain-torsa] ca identifier myca
```

# Configure the certificate request URL. The URL is in the format **http://host:port/Issuing Jurisdiction ID**, where *Issuing Jurisdiction ID* is a hexadecimal string generated on the CA server.

```
[DeviceA-pki-domain-torsa] certificate request url
http://[3001::5]:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

# Configure the device to send certificate requests to **ca**.

```
[DeviceA-pki-domain-torsa] certificate request from ca
```

# Set the PKI entity name to **aaa**.

```
[DeviceA-pki-domain-torsa] certificate request entity aaa
```

# Specify the URL of the CRL repository. In this example, the URL in HTTP format is not allowed because the RSA Keon CA server cannot process IPv6 data in HTTP packets, although IPv6 packets from Device A can be converted to IPv4 packets by Device B. If an OpenCA server acts as the CA server, you can specify a URL in HTTP format. This limitation depends on the types of your CA server.

```
[DeviceA-pki-domain-torsa] crl url
ldap://[3001::5]:389/CN=sslrsa,OU=sec,O=docm,C=cn
```

# Configure a general-purpose RSA key pair named **abc** with a length of 1024 bits.

```
[DeviceA-pki-domain-torsa] public-key rsa general name abc length 1024
[DeviceA-pki-domain-torsa] quit
```

#### 4. Generate the RSA key pair.

```
[DeviceA] public-key local create rsa name abc
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....++++++

.....++++++

Create the key pair successfully.

#### 5. Request a local certificate:

# Obtain the CA certificate and save it locally.

```
[DeviceA] pki retrieve-certificate domain torsa ca
```

The trusted CA's finger print is:

MD5 fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB

SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

Is the finger print correct?(Y/N):y

Retrieved the certificates successfully

# Obtain the CRL and save it locally.

```
[DeviceA] pki retrieve-crl domain torsa
```

# Submit a certificate request manually.

```
[DeviceA] pki request-certificate domain torsa password 123
```

Start to request the general certificate ...

...

Request certificate of domain torsa successfully

### Verifying the configuration

# Display information about the local certificate in PKI domain **torsa**.

```
[DeviceA] display pki certificate domain torsa local
```

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
 1a:6f:8e:6c:d6:36:b9:00:37:51:19:f5:ad:e7:30:e2
Signature Algorithm: sha1WithRSAEncryption
Issuer: CN=myca
Validity
 Not Before: Jan 6 03:18:53 2013 GMT
 Not After : Jan 6 03:18:53 2014 GMT
Subject: CN=test
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (1024 bit)
 Modulus:
 00:b8:65:45:a1:5e:21:e3:c0:c4:25:e5:26:97:25:
 f8:91:c5:3c:76:95:2c:34:66:1a:4c:af:bc:0a:92:
 9d:c2:79:ec:2d:eb:5a:3a:54:e1:98:e6:c1:58:ee:
 0f:4b:84:63:51:d8:37:a5:a5:fd:7e:81:1f:d2:8c:
 53:a3:09:3e:98:a8:51:d5:3f:3c:02:02:d3:19:51:
 ca:6c:a0:a1:4d:07:0d:d8:09:61:6f:dd:10:e5:0f:
 18:4d:43:e6:43:ec:54:c6:ba:2e:b5:c4:dc:ba:05:
 53:74:e8:e9:42:ef:c6:9d:98:b7:1c:20:c7:03:a9:
 f2:26:64:a6:ad:05:09:c8:69
 Exponent: 65537 (0x10001)
X509v3 extensions:
 X509v3 CRL Distribution Points:

 Full Name:
 DirName: CN = myca
```

```
Signature Algorithm: sha1WithRSAEncryption
6e:91:d6:74:f6:b7:60:a7:0d:c9:d8:6f:a2:c6:04:a2:d0:1b:
23:8b:5e:3d:66:00:03:5e:15:f0:42:58:d1:8c:e3:54:8e:de:
2f:7c:fa:f2:8b:bf:c0:c4:a0:1c:d2:04:3e:b9:39:1e:16:34:
4a:ef:b1:10:96:60:aa:5c:c0:5a:b3:26:9d:dc:f9:57:ec:9d:
6c:31:be:bb:af:40:a9:b1:a6:98:ca:cd:a0:f0:e7:10:4e:6e:
b1:d8:ab:15:37:e6:83:12:21:1f:a8:c0:a8:23:1f:07:aa:0a:
fc:be:ce:20:e4:55:79:51:8f:ec:02:12:92:23:9e:cf:14:5c:
39:43
```

To display detailed information about the CA certificate and the CRLs, use the **display pki certificate domain** and **display pki crl domain** commands.

## IKE negotiation with RSA digital signature from a Windows Server 2003 CA server

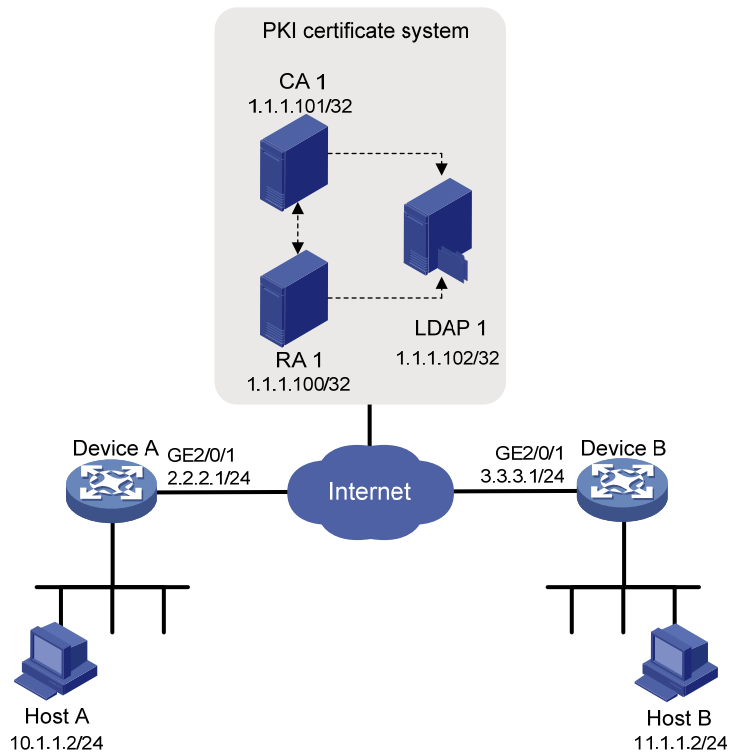
### Network requirements

As shown in [Figure 93](#), an IPsec tunnel is established between Device A and Device B to protect the traffic between Host A on subnet 10.1.1.0/24 and Host B on subnet 1.1.1.0/24.

Device A and Device B use IKE to set up SAs, and the IKE proposal uses RSA digital signature for identity authentication.

Device A and Device B use the same CA.

**Figure 93 Network diagram**



## Configuring the Windows Server 2003 CA server

See "[Requesting a certificate from a Windows Server 2003 CA server.](#)"

## Configuring Device A

# Configure a PKI entity.

```
<DeviceA> system-view
[DeviceA] pki entity en
[DeviceA-pki-entity-en] ip 2.2.2.1
[DeviceA-pki-entity-en] common-name devicea
[DeviceA-pki-entity-en] quit
```

# Configure a PKI domain.

```
[DeviceA] pki domain 1
[DeviceA-pki-domain-1] ca identifier CA1
[DeviceA-pki-domain-1] certificate request url http://1.1.1.100/certsrv/mscep/mscep.dll
[DeviceA-pki-domain-1] certificate request entity en
[DeviceA-pki-domain-1] ldap-server host 1.1.1.102
```

# Configure the device to send certificate requests to **ra**.

```
[DeviceA-pki-domain-1] certificate request from ra
```

# Configure a general-purpose RSA key pair named **abc** with a length of 1024 bits.

```
[DeviceA-pki-domain-1] public-key rsa general name abc length 1024
[DeviceA-pki-domain-1] quit
```

# Generate the RSA key pair.

```

[DeviceA] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
Create the key pair successfully.
Obtain the CA certificate and save it locally.
[DeviceA] pki retrieve-certificate domain 1 ca
Submit a certificate request manually.
[DeviceA] pki request-certificate domain 1
Create IKE proposal 1, and configure the authentication method as RSA digital signature.
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method rsa-signature
[DeviceA-ike-proposal-1] quit
Reference the PKI domain used in IKE negotiation for the IKE profile peer.
[DeviceA] ike profile peer
[DeviceA-ike-profile-peer] certificate domain 1

```

## Configuring Device B

```

Configure a PKI entity.
<DeviceB> system-view
[DeviceB] pki entity en
[DeviceB-pki-entity-en] ip 3.3.3.1
[DeviceB-pki-entity-en] common-name deviceb
[DeviceB-pki-entity-en] quit
Configure a PKI domain.
[DeviceB] pki domain 1
[DeviceB-pki-domain-1] ca identifier CA1
[DeviceB-pki-domain-1] certificate request url http://1.1.1.100/certsrv/mscep/mscep.dll
[DeviceB-pki-domain-1] certificate request entity en
[DeviceB-pki-domain-1] ldap-server host 1.1.1.102
Configure the device to send certificate requests to ra.
[DeviceB-pki-domain-1] certificate request from ra
Configure a general-purpose RSA key pair named abc with a length of 1024 bits.
[DeviceB-pki-domain-1] public-key rsa general name abc length 1024
[DeviceB-pki-domain-1] quit
Generate the RSA key pair.
[DeviceB] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++

```



```

.....+++++
Create the key pair successfully.
Obtain the CA certificate and save it locally.
[DeviceB] pki retrieve-certificate ca domain 1
Submit a certificate request manually.
[DeviceB] pki request-certificate domain 1
Create IKE proposal 1, and configure the authentication method as RSA digital signature.
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method rsa-signature
[DeviceB-ike-proposal-1] quit
Reference the PKI domain used in IKE negotiation for the IKE profile peer.
[DeviceB] ike profile peer
[DeviceB-ike-profile-peer] certificate domain 1

The configurations are for IKE negotiation with RSA digital signature. For information about how to
configure IPsec SAs to be set up, see "Configuring IPsec."

```

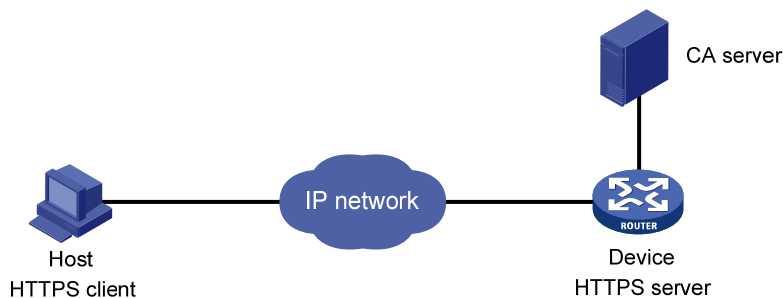
## Certificate-based access control policy configuration example

### Network requirements

As shown in [Figure 94](#), the host accesses the device through HTTPS.

Configure a certificate-based access control policy on the device to authenticate the host and verify the validity of the host's certificate.

**Figure 94 Network diagram**



### Configuration procedure

1. Create the PKI domain **domain1** to be referenced by SSL. (Details not shown.)
2. Request an SSL server certificate for the device from the CA server. (Details not shown.)
3. Configure the HTTPS server (the device):
  - # Enable the HTTPS services.
  - <Device> system-view
  - [Device] ip https enable
  - # Configure an SSL policy for the HTTPS server.
  - [Device] ssl server-policy abc
  - [Device-ssl-server-policy-abc] pki-domain domain1
  - [Device-ssl-server-policy-abc] client-verify enable
  - [Device-ssl-server-policy-abc] quit

4. Configure certificate attribute groups:

# Create a certificate attribute group named **mygroup1** and add two attribute rules. The first rule defines that the DN in the subject DN contains the string of **aabbcc**. The second rule defines that the IP address of the certificate issuer is **10.0.0.1**.

```
[Device] pki certificate attribute-group mygroup1
[Device-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
[Device-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
[Device-pki-cert-attribute-group-mygroup1] quit
```

# Create a certificate attribute group named **mygroup2** and add two attribute rules. The first rule defines that the FQDN in the alternative subject name does not contain the string of **apple**. The second rule defines that the DN of the certificate issuer name contains the string of **aabbcc**.

```
[Device] pki certificate attribute-group mygroup2
[Device-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
[Device-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
[Device-pki-cert-attribute-group-mygroup2] quit
```

5. Configure a certificate-based access control policy:

# Create a certificate-based access control policy named **myacp**.

```
[Device] pki certificate access-control-policy myacp
```

# Define a statement to deny the certificates that match the attribute rules in the certificate attribute group **mygroup1**.

```
[Device-pki-cert-acp-myacp] rule 1 deny mygroup1
```

# Define a statement to permit the certificates that match the attribute rules in the certificate attribute group **mygroup2**.

```
[Device-pki-cert-acp-myacp] rule 2 permit mygroup2
```

```
[Device-pki-cert-acp-myacp] quit
```

## Verifying the configuration

# On the host, access the HTTPS server through a Web browser.

The server first verifies the validity of the host's certificate according to the configured certificate-based access control policy. In the host's certificate, the subject DN is **aabbcc**, the IP address of the certificate issuer is **1.1.1.1**, and the FQDN of the alternative subject name is **banaba**.

The host's certificate does not match the certificate attribute group **mygroup1** specified in **rule 1** of the certificate-based access control policy. The certificate continues to match against rule 2.

The host's certificate matches the certificate attribute group **mygroup2** specified in **rule 2**. Because **rule 2** is a permit statement, the certificate passes the verification and the host can access the HTTPS server.

## Certificate import and export configuration example

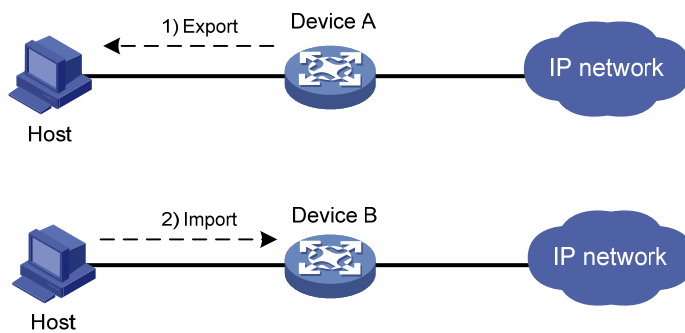
### Network requirements

As shown in [Figure 95](#), Device B will replace Device A in the network. The PKI domain **exportdomain** on Device A has two local certificates containing the private key and one CA certificate. To make sure the certificates are still valid after Device B replaces Device A, copy the certificates on Device A to Device B as follows:

1. Export the certificates in PKI domain **exportdomain** on Device A to .pem certificate files.  
During the export, encrypt the private key in the local certificates using 3DES\_CBC with the password 11111.
2. Transfer the certificate files from Device A to Device B through the FTP host.

3. Import the certificate files to PKI domain **importdomain** on Device B.

**Figure 95 Network diagram**



## Configuration procedure

1. Export the certificates on Device A:

# Export the CA certificate to a .pem file.

```
<DeviceA> system-view
```

```
[DeviceA] pki export domain exportdomain pem ca filename pkicachain.pem
```

# Export the local certificate to a file named **pkilocal.pem** in PEM format, and use 3DES\_CBC to encrypt the private key with the password **111111**.

```
[DeviceA] pki export domain exportdomain pem local 3des-cbc 111111 filename pkilocal.pem
```

Now, Device A has three certificate files in PEM format:

- A CA certificate file named **pkicachain.pem**.
- A local certificate file named **pkilocal.pem-signature**, which contains the private key for signature.
- A local certificate file named **pkilocal.pem-encryption**, which contains the private key for encryption.

# Display the local certificate file **pkilocal.pem-signature**.

```
[DeviceA] quit
```

```
<DeviceA> more pkicachain.pem-sign
```

Bag Attributes

friendlyName:

localKeyID: 90 C6 DC 1D 20 49 4F 24 70 F5 17 17 20 2B 9E AC 20 F3 99 89

subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subsign 11

issuer=/C=CN/L=shangdi/ST=pukras/O=OpenCA Labs/OU=docm/CN=subca1

-----BEGIN CERTIFICATE-----

MIIEGjCCA2qgAwIBAgILAJgsebpejZc5UwAwDQYJKoZIhvcNAQELBQAwZjELMAkG

...

-----END CERTIFICATE-----

Bag Attributes

friendlyName:

localKeyID: 90 C6 DC 1D 20 49 4F 24 70 F5 17 17 20 2B 9E AC 20 F3 99 89

Key Attributes: <No Attributes>

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIICxjBAbGkqhkiG9w0BBQowMzAbBgkqhkiG9w0BBQwwDgQIZtjSjfsLJCoCAggA

...

-----END ENCRYPTED PRIVATE KEY-----

# Display the local certificate file **pkilocal.pem-encryption**.

```
<DeviceA> more pkicachain.pem-encr
Bag Attributes
 friendlyName:
 localKeyID: D5 DF 29 28 C8 B9 D9 49 6C B5 44 4B C2 BC 66 75 FE D6 6C C8
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subencr 11
issuer=/C=CN/L=shangdi/ST=pukras/O=OpenCA Labs/OU=docm/CN=subca1
-----BEGIN CERTIFICATE-----
MIEUDCCAzigAwIBAgIKCHxnAVyzWhIPLzANBgkqhkiG9w0BAQsFADBmMQswCQYD
...
-----END CERTIFICATE-----
Bag Attributes
 friendlyName:
 localKeyID: D5 DF 29 28 C8 B9 D9 49 6C B5 44 4B C2 BC 66 75 FE D6 6C C8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI7H0mb407/GACAggA
...
-----END ENCRYPTED PRIVATE KEY-----
```

2. Download the certificate files **pkicachain.pem**, **pkilocal.pem-sign**, and **pkilocal.pem-encr** from Device A to the host through FTP. (Details not shown.)
3. Upload the certificate files **pkicachain.pem**, **pkilocal.pem-sign**, and **pkilocal.pem-encr** from the host to Device B through FTP. (Details not shown.)
4. Import the certificate files to Device B:

# Disable CRL checking. (You can configure CRL checking as required. This example assumes CRL checking is not required.)

```
<DeviceB> system-view
```

```
[DeviceB] pki domain importdomain
```

```
[DeviceB-pki-domain-importdomain] undo crl check enable
```

# Specify the RSA key pair for signature as **sign**, and the RSA key pair for encryption as **encr** for certificate request.

```
[DeviceB-pki-domain-importdomain] public-key rsa signature name sign encryption name encr
```

```
[DeviceB-pki-domain-importdomain] quit
```

# Import the CA certificate file **pkicachain.pem** in PEM format to the PKI domain.

```
[DeviceB] pki import domain importdomain pem ca filename pkicachain.pem
```

# Import the local certificate file **pkilocal.pem-signature** in PEM format to the PKI domain. The certificate file contains a key pair.

```
[DeviceB] pki import domain importdomain pem local filename pkilocal.pem-signature
Please input the password:*****
```

# Import the local certificate file **pkilocal.pem-encryption** in PEM format to the PKI domain. The certificate file contains a key pair.

```
[DeviceB] pki import domain importdomain pem local filename pkilocal.pem-encryption
Please input the password:*****
```

# Display the imported local certificate information on Device B.

```
[DeviceB] display pki certificate domain importdomain local
```

Certificate:

Data:

Version: 3 (0x2)

```

Serial Number:
 98:2c:79:ba:5e:8d:97:39:53:00
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CN, L=shangdi, ST=pukras, O=OpenCA Labs, OU=docm, CN=subca1
Validity
 Not Before: May 26 05:56:49 2011 GMT
 Not After : Nov 22 05:56:49 2012 GMT
Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subsign 11
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (1024 bit)
 Modulus:
 00:9f:6e:2f:f6:cb:3d:08:19:9a:4a:ac:b4:ac:63:
 ce:8d:6a:4c:3a:30:19:3c:14:ff:a9:50:04:f5:00:
 ee:a3:aa:03:cb:b3:49:c4:f8:ae:55:ee:43:93:69:
 6c:bf:0d:8c:f4:4e:ca:69:e5:3f:37:5c:83:ea:83:
 ad:16:b8:99:37:cb:86:10:6b:a0:4d:03:95:06:42:
 ef:ef:0d:4e:53:08:0a:c9:29:dd:94:28:02:6e:e2:
 9b:87:c1:38:2d:a4:90:a2:13:5f:a4:e3:24:d3:2c:
 bf:98:db:a7:c2:36:e2:86:90:55:c7:8c:c5:ea:12:
 01:31:69:bf:e3:91:71:ec:21
 Exponent: 65537 (0x10001)
X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Cert Type:
 SSL Client, S/MIME
 X509v3 Key Usage:
 Digital Signature, Non Repudiation
 X509v3 Extended Key Usage:
 TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
 Netscape Comment:
 User Certificate of OpenCA Labs
 X509v3 Subject Key Identifier:
 AA:45:54:29:5A:50:2B:89:AB:06:E5:BD:0D:07:8C:D9:79:35:B1:F5
 X509v3 Authority Key Identifier:
 keyid:70:54:40:61:71:31:02:06:8C:62:11:0A:CC:A5:DB:0E:7E:74:DE:DD

 X509v3 Subject Alternative Name:
 email:subsign@docm.com
 X509v3 Issuer Alternative Name:
 DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1
Authority Information Access:
 CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
 OCSP - URI:http://titan:2560/
 1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

```

X509v3 CRL Distribution Points:

Full Name:

URI:http://192.168.40.130/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption

18:e7:39:9a:ad:84:64:7b:a3:85:62:49:e5:c9:12:56:a6:d2:  
46:91:53:8e:84:ba:4a:0a:6f:28:b9:43:bc:e7:b0:ca:9e:d4:  
1f:d2:6f:48:c4:b9:ba:c5:69:4d:90:f3:15:c4:4e:4b:1e:ef:  
2b:1b:2d:cb:47:1e:60:a9:0f:81:dc:f2:65:6b:5f:7a:e2:36:  
29:5d:d4:52:32:ef:87:50:7c:9f:30:4a:83:de:98:8b:6a:c9:  
3e:9d:54:ee:61:a4:26:f3:9a:40:8f:a6:6b:2b:06:53:df:b6:  
5f:67:5e:34:c8:c3:b5:9b:30:ee:01:b5:a9:51:f9:b1:29:37:  
02:1a:05:02:e7:cc:1c:fe:73:d3:3e:fa:7e:91:63:da:1d:f1:  
db:28:6b:6c:94:84:ad:fc:63:1b:ba:53:af:b3:5d:eb:08:b3:  
5b:d7:22:3a:86:c3:97:ef:ac:25:eb:4a:60:f8:2b:a3:3b:da:  
5d:6f:a5:cf:cb:5a:0b:c5:2b:45:b7:3e:6e:39:e9:d9:66:6d:  
ef:d3:a0:f6:2a:2d:86:a3:01:c4:94:09:c0:99:ce:22:19:84:  
2b:f0:db:3e:1e:18:fb:df:56:cb:6f:a2:56:35:0d:39:94:34:  
6d:19:1d:46:d7:bf:1a:86:22:78:87:3e:67:fe:4b:ed:37:3d:  
d6:0a:1c:0b

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

08:7c:67:01:5c:b3:5a:12:0f:2f

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=CN, L=shangdi, ST=pukras, O=OpenCA Labs, OU=docm, CN=subca1

Validity

Not Before: May 26 05:58:26 2011 GMT

Not After : Nov 22 05:58:26 2012 GMT

Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subencr 11

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:db:26:13:d3:d1:a4:af:11:f3:6d:37:cf:d0:d4:  
48:50:4e:0f:7d:54:76:ed:50:28:c6:71:d4:48:ae:  
4d:e7:3d:23:78:70:63:18:33:f6:94:98:aa:fa:f6:  
62:ed:8a:50:c6:fd:2e:f4:20:0c:14:f7:54:88:36:  
2f:e6:e2:88:3f:c2:88:1d:bf:8d:9f:45:6c:5a:f5:  
94:71:f3:10:e9:ec:81:00:28:60:a9:02:bb:35:8b:  
bf:85:75:6f:24:ab:26:de:47:6c:ba:1d:ee:0d:35:  
75:58:10:e5:e8:55:d1:43:ae:85:f8:ff:75:81:03:  
8c:2e:00:d1:e9:a4:5b:18:39

Exponent: 65537 (0x10001)

X509v3 extensions:

```

X509v3 Basic Constraints:
 CA:FALSE
Netscape Cert Type:
 SSL Server
X509v3 Key Usage:
 Key Encipherment, Data Encipherment
Netscape Comment:
 VPN Server of OpenCA Labs
X509v3 Subject Key Identifier:
 CC:96:03:2F:FC:74:74:45:61:38:1F:48:C0:E8:AA:18:24:F0:2B:AB
X509v3 Authority Key Identifier:
 keyid:70:54:40:61:71:31:02:06:8C:62:11:0A:CC:A5:DB:0E:7E:74:DE:DD

X509v3 Subject Alternative Name:
 email:subencr@docm.com
X509v3 Issuer Alternative Name:
 DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1
Authority Information Access:
 CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
 OCSP - URI:http://titan:2560/
 1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

X509v3 CRL Distribution Points:

 Full Name:
 URI:http://192.168.40.130/pki/pub/crl/cacrl.crl

```

```

Signature Algorithm: sha256WithRSAEncryption
53:69:66:5f:93:f0:2f:8c:54:24:8f:a2:f2:f1:29:fa:15:16:
90:71:e2:98:e3:5c:c6:e3:d4:5f:7a:f6:a9:4f:a2:7f:ca:af:
c4:c8:c7:2c:c0:51:0a:45:d4:56:e2:81:30:41:be:9f:67:a1:
23:a6:09:50:99:a1:40:5f:44:6f:be:ff:00:67:9d:64:98:fb:
72:77:9e:fd:f2:4c:3a:b2:43:d8:50:5c:48:08:e7:77:df:fb:
25:9f:4a:ea:de:37:1e:fb:bc:42:12:0a:98:11:f2:d9:5b:60:
bc:59:72:04:48:59:cc:50:39:a5:40:12:ff:9d:d0:69:3a:5e:
3a:09:5a:79:e0:54:67:a0:32:df:bf:72:a0:74:63:f9:05:6f:
5e:28:d2:e8:65:49:e6:c7:b5:48:7d:95:47:46:c1:61:5a:29:
90:65:45:4a:88:96:e4:88:bd:59:25:44:3f:61:c6:b1:08:5b:
86:d2:4f:61:4c:20:38:1c:f4:a1:0b:ea:65:87:7d:1c:22:be:
b6:17:17:8a:5a:0f:35:4c:b8:b3:73:03:03:63:b1:fc:c4:f5:
e9:6e:7c:11:e8:17:5a:fb:39:e7:33:93:5b:2b:54:72:57:72:
5e:78:d6:97:ef:b8:d8:6d:0c:05:28:ea:81:3a:06:a0:2e:c3:
79:05:cd:c3

```

To display detailed information about the CA certificate, use the **display pki certificate domain** command.

# Troubleshooting PKI configuration

This section provides troubleshooting information for common problems with PKI.

## Failed to obtain the CA certificate

### Symptom

The CA certificate cannot be obtained.

### Analysis

- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No trusted CA is specified.
- The certificate request URL is incorrect or not specified.
- The system time of the device is not synchronized with the CA server.
- The source IP address of the PKI protocol packets is not specified or is incorrect.
- The fingerprint of the root CA certificate is illegal.

### Solution

1. Check for and fix any network connection problems.
2. Verify that the required configurations are correct.
3. Use **ping** to verify that the registration server is reachable.
4. Synchronize the system time of the device with the CA server.
5. Specify the correct source IP address for PKI protocol packets that the CA server can accept.
6. Verify the CA certificate's fingerprint on the CA server.
7. If the problem persists, contact Hewlett Packard Enterprise Support.

## Failed to obtain local certificates

### Symptom

No local certificates can be obtained.

### Analysis

- The network connection is down.
- No CA certificate has been obtained before you try to obtain local certificates.
- The LDAP server is not configured or is incorrectly configured.
- No key pair is specified for the PKI domain for certificate request, or the specified key pair does not match the local certificates to be obtained.
- The PKI domain does not reference the PKI entity configuration, or the PKI entity configuration is incorrect.
- CRL checking is enabled, but CRLs do not exist locally or CRLs cannot be obtained.
- The CA server does not accept the source IP address specified in the PKI domain, or the source IP address is incorrect.
- The system time of the device is not synchronized with the CA server.

### Solution

1. Check for and fix any network connection problems.



2. Obtain or import the CA certificate.
3. Configure the correct LDAP server.
4. Specify the key pair used for certificate request in the PKI domain, or remove the existing key pair and submit a certificate request again.
5. Check the registration policy on the CR or RA, and make sure the attributes of the PKI entity meet the policy requirements.
6. Obtain the CRL from the CRL repository.
7. Specify the correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
8. Synchronize the system time of the device with the CA server.
9. If the problem persists, contact Hewlett Packard Enterprise Support.

## Failed to request local certificates

### Symptom

Local certificate requests cannot be submitted.

### Analysis

- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No CA certificate has been obtained before you submit the certificate request.
- The certificate request URL is incorrect or is not specified.
- The certificate request reception authority is incorrect or is not specified.
- The required parameters are not configured for the PKI entity or are mistakenly configured.
- No key pair is specified for the PKI domain for certificate request, or the key pair is changed during a certificate request process.
- Exclusive certificate request applications are running in the PKI domain.
- The PKI domain is not specified with the source IP address that the CA server can accept, or is specified with an incorrect one.
- The system time of the device is not synchronized with the CA server.

### Solution

1. Check for and fix any network connection problems.
2. Obtain or import the CA certificate.
3. Use **ping** to verify that the registration server is reachable.
4. Specify the correct certificate request URL.
5. Check the registration policy on the CR or RA, and make sure the attributes of the PKI entity meet the policy requirements.
6. Specify the key pair used for certificate request in the PKI domain, or remove the key pair specified in the PKI and submit a certificate request again.
7. Use **pki abort-certificate-request domain** to abort the certificate request.
8. Specify the correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
9. Synchronize the system time of the device with the CA server.
10. If the problem persists, contact Hewlett Packard Enterprise Support.

# Failed to obtain CRLs

## Symptom

CRLs cannot be obtained.

## Analysis

- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No CA certificate has been obtained before you try to obtain CRLs.
- The URL of the CRL repository is not configured and cannot be obtained from the CA certificate or local certificates in the PKI domain.
- The specified URL of the CRL repository is incorrect.
- The device tries to obtain CRLs through SCEP, but experiences the following problems:
  - The PKI domain does not have local certificates.
  - The key pairs in the certificates have been changed.
  - The PKI domain has incorrect URL for certificate request.
- The specified URL of the CRL repository does not contain the host name or IP address, and the LDAP server is incorrect or is not specified in the PKI domain.
- The CA does not issue CRLs.
- The PKI domain is not specified with the source IP address that the CA server can accept, or is specified with an incorrect one.

## Solution

1. Check for and fix any network connection problems.
2. Obtain or import the CA certificate.
3. If the URL of the CRL repository cannot be obtained, verify that the following conditions exist:
  - The URL for certificate request is valid.
  - A local certificate has been successfully obtained.
  - The local certificate contains a public key that matches the locally stored key pair.
4. Make sure the LDAP server address is contained in the CRL repository URL, or is configured in the PKI domain.
5. Make sure the CA server support publishing CRLs.
6. Specify a correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
7. If the problem persists, contact Hewlett Packard Enterprise Support.

# Failed to import the CA certificate

## Symptom

The CA certificate cannot be imported.

## Analysis

- CRL checking is enabled, but the device does not have a locally stored CRL and cannot obtain one.
- The specified format does not match the actual format of the file to be imported.

## Solution

1. Use **undo crl check enable** to disable CRL checking.

2. Make sure the format of the imported file is correct.
3. If the problem persists, contact Hewlett Packard Enterprise Support.

## Failed to import a local certificate

### Symptom

A local certificate cannot be imported.

### Analysis

- The PKI domain has no CA certificate, and the certificate file to be imported does not contain the CA certificate chain.
- CRL checking is enabled, but the device does not have a locally stored CRL and cannot obtain one.
- The specified format does not match the actual format of the file to be imported.
- The device and the certificate do not have the local key pair.
- The certificate has been revoked.
- The certificate is out of the validity period.
- The system time is wrong.

### Solution

1. Obtain or import the CA certificate.
2. Use **undo crl check enable** to disable CRL checking, or obtain the correct CRL before you import certificates.
3. Make sure the format of the file to be imported is correct.
4. Make sure the certificate file contains the private key.
5. Make sure the certificate is not revoked.
6. Make sure the certificate is valid.
7. Configure the correct system time for the device.
8. If the problem persists, contact Hewlett Packard Enterprise Support.

## Failed to export certificates

### Symptom

Certificates cannot be exported.

### Analysis

- The PKI domain does not have local certificates when you export all certificates in PKCS12 format.
- The specified export path does not exist.
- The specified export path is illegal.
- The public key of the local certificate to be exported does not match the public key in the key pair of the PKI domain.
- The storage space of the device is full.

### Solution

1. If the PKI domain does not have local certificates, obtain or request local certificates first.
2. Use **mkdir** to create the required path.
3. Specify a correct export path.

4. Configure the correct key pair in the PKI domain.
5. Clear up the storage space of the device.
6. If the problem persists, contact Hewlett Packard Enterprise Support.

## Failed to set the storage path

### Symptom

The storage path for certificates or CRLs cannot be set.

### Analysis

- The specified storage path does not exist.
- The specified storage path is illegal.
- The storage space of the device is full.

### Solution

1. Use **mkdir** to create the path.
2. Specify a valid storage path for certificates or CRLs.
3. Clear up the storage space of the device.
4. If the problem persists, contact Hewlett Packard Enterprise Support.

# Configuring IPsec

## Overview

IP Security (IPsec) is defined by the IETF to provide interoperable, high-quality, cryptography-based security for IP communications. It is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

IPsec is a security framework that has the following protocols and algorithms:

- Authentication Header (AH).
- Encapsulating Security Payload (ESP).
- Internet Key Exchange (IKE).
- Algorithms for authentication and encryption.

AH and ESP are security protocols that provide security services. IKE performs automatic key exchange. For more information about IKE, see "[Configuring IKE](#)."

IPsec provides the following security services for data packets in the IP layer:

- **Confidentiality**—The sender encrypts packets before transmitting them over the Internet, protecting the packets from being eavesdropped en route.
- **Data integrity**—The receiver verifies the packets received from the sender to make sure they are not tampered with during transmission.
- **Data origin authentication**—The receiver verifies the authenticity of the sender.
- **Anti-replay**—The receiver examines packets and drops outdated and duplicate packets.

IPsec delivers the following benefits:

- Reduced key negotiation overhead and simplified maintenance by supporting the IKE protocol. IKE provides automatic key negotiation and automatic IPsec security association (SA) setup and maintenance.
- Good compatibility. You can apply IPsec to all IP-based application systems and services without modifying them.
- Encryption on a per-packet rather than per-flow basis. Per-packet encryption allows for flexibility and greatly enhances IP security.

## Security protocols and encapsulation modes

### Security protocols

IPsec comes with two security protocols, AH and ESP. They define how to encapsulate IP packets and the security services that they can provide.

- AH (protocol 51) defines the encapsulation of the AH header in an IP packet, as shown in [Figure 98](#). AH can provide data origin authentication, data integrity, and anti-replay services to prevent data tampering, but it cannot prevent eavesdropping. Therefore, it is suitable for transmitting non-confidential data. AH supports authentication algorithms HMAC-MD5 and HMAC-SHA1.
- ESP (protocol 50) defines the encapsulation of the ESP header and trailer in an IP packet, as shown in [Figure 98](#). ESP can provide data encryption, data origin authentication, data integrity, and anti-replay services. Unlike AH, ESP can guarantee data confidentiality because it can encrypt the data before encapsulating the data to IP packets. ESP supports encryption

algorithms such as DES, 3DES, and AES, and authentication algorithms HMAC-MD5 and HMAC-SHA1.

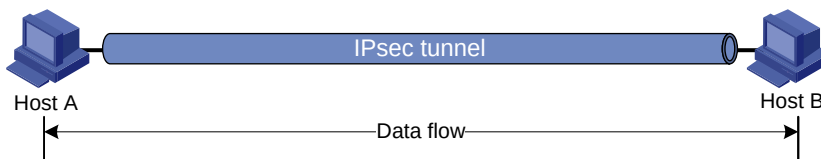
Both AH and ESP provide authentication services, but the authentication service provided by AH is stronger. In practice, you can choose either or both security protocols. When both AH and ESP are used, an IP packet is encapsulated first by ESP and then by AH.

## Encapsulation modes

IPsec supports the following encapsulation modes:

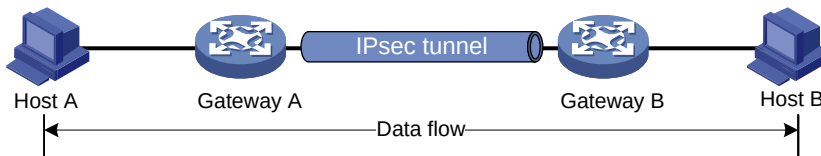
- Transport mode**—The security protocols protect the upper layer data of an IP packet. Only the transport layer data is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are placed after the original IP header. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications, as shown in [Figure 96](#).

**Figure 96 IPsec protection in transport mode**



- Tunnel mode**—The security protocols protect the entire IP packet. The entire IP packet is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are encapsulated in a new IP packet. In this mode, the encapsulated packet has two IP headers. The inner IP header is the original IP header. The outer IP header is added by the network device that provides the IPsec service. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications, as shown in [Figure 97](#).

**Figure 97 IPsec protection in tunnel mode**



[Figure 98](#) shows how the security protocols encapsulate an IP packet in different encapsulation modes.

**Figure 98 Security protocol encapsulations in different modes**

| Mode<br>Protocol | Transport            | Tunnel                  |
|------------------|----------------------|-------------------------|
| AH               | IP AH Data           | IP AH IP Data           |
| ESP              | IP ESP Data ESP-T    | IP ESP IP Data ESP-T    |
| AH-ESP           | IP AH ESP Data ESP-T | IP AH ESP IP Data ESP-T |

# Security association

A security association (SA) is an agreement negotiated between two communicating parties called IPsec peers. An SA comprises the following parameters for data protection:

- Security protocols (AH, ESP, or both).
- Encapsulation mode (transport mode or tunnel mode).
- Authentication algorithm (HMAC-MD5 or HMAC-SHA1).
- Encryption algorithm (DES, 3DES, or AES).
- Shared keys and their lifetimes.

An SA is unidirectional. At least two SAs are needed to protect data flows in a bidirectional communication. If two peers want to use both AH and ESP to protect data flows between them, they construct an independent SA for each protocol in each direction.

An SA is uniquely identified by a triplet, which consists of the security parameter index (SPI), destination IP address, and security protocol identifier. An SPI is a 32-bit number. It is transmitted in the AH/ESP header.

An SA can be set up manually or through IKE.

- **Manual mode**—Configure all parameters for the SA through commands. This configuration mode is complex and does not support some advanced features (such as periodic key update), but it can implement IPsec without IKE. This mode is mainly used in small and static networks or when the number of IPsec peers in the network is small.
- **IKE negotiation mode**—The peers negotiate and maintain the SA through IKE. This configuration mode is simple and has good expansibility. As a best practice, set up SAs through IKE negotiations in medium- and large-scale dynamic networks.

A manually configured SA never ages out. An IKE-created SA has a lifetime, which comes in two types:

- **Time-based lifetime**—Defines how long the SA can be valid after it is created.
- **Traffic-based lifetime**—Defines the maximum traffic that the SA can process.

If both lifetime timers are configured for an SA, the SA becomes invalid when either of the lifetime timers expires. Before the SA expires, IKE negotiates a new SA, which takes over immediately after its creation.

## Authentication and encryption

### Authentication algorithms

IPsec uses hash algorithms to perform authentication. A hash algorithm produces a fixed-length digest for an arbitrary-length message. IPsec peers respectively calculate message digests for each packet. The receiver compares the local digest with that received from the sender. If the digests are identical, the receiver considers the packet intact and the sender's identity valid. IPsec uses the Hash-based Message Authentication Code (HMAC) based authentication algorithms, including HMAC-MD5 and HMAC-SHA1. Compared with HMAC-SHA1, HMAC-MD5 is faster but less secure.

### Encryption algorithms

IPsec uses symmetric encryption algorithms, which encrypt and decrypt data by using the same keys. The following encryption algorithms are available for IPsec on the device:

- **DES**—Encrypts a 64-bit plaintext block with a 56-bit key. DES is the least secure but the fastest algorithm.
- **3DES**—Encrypts plaintext data with three 56-bit DES keys. The key length totals up to 168 bits. It provides moderate security strength and is slower than DES.

- **AES**—Encrypts plaintext data with a 128-bit, 192-bit, or 256-bit key. AES provides the highest security strength and is slower than 3DES.

## Crypto engine

The IPsec feature is resource intensive for its complex encryption/decryption and authentication algorithms. To improve processing performance, you can use crypto engine to offload IPsec tasks.

The crypto engine processes all IPsec protected packets and hands the processed packets back to the device for forwarding.

For more information about crypto engines, see "[Configuring crypto engines](#)."

## IPsec implementation

To implement IPsec protection for packets between two peers, complete the following tasks on each peer:

- Configure an IPsec policy, which defines the range of packets to be protected by IPsec and the security parameters used for the protection.
- Apply the IPsec policy to an interface or an application.

When you apply an IPsec policy to an interface, you implement IPsec based on the interface. Packets received and sent by the interface are protected according to the IPsec policy. When you apply an IPsec policy to an application, you implement IPsec based on the application. Packets of the application are protected according to the IPsec policy, regardless of the receiving and sending interface of the packets.

IPsec protects packets as follows:

- When an IPsec peer identifies the packets to be protected according to the IPsec policy, it sets up an IPsec tunnel and sends the packet to the remote peer through the tunnel. The IPsec tunnel can be manually configured beforehand, or it can be set up through IKE negotiation triggered by the packet. The IPsec tunnels are actually the IPsec SAs. The inbound packets are protected by the inbound SA, and the outbound packets are protected by the outbound SA.
- When the remote IPsec peer receives the packet, it drops, de-encapsulates, or directly forwards the packet according to the configured IPsec policy.

Interface-based IPsec supports setting up IPsec tunnels based on ACLs.

## ACL-based IPsec

To implement ACL-based IPsec, configure an ACL to define the data flows to be protected, specify the ACL in an IPsec policy, and then apply the IPsec policy to an interface. When packets sent by the interface match the permit rule of the ACL, the packets are protected by the outbound IPsec SA and encapsulated with IPsec. When the interface receives an IPsec packet whose destination address is the IP address of the local device, it searches for the inbound IPsec SA according to the SPI carried in the IPsec packet header for de-encapsulation. If the de-encapsulated packet matches the permit rule of the ACL, the device processes the packet. Otherwise, it drops the packet.

The device supports the following data flow protection modes:

- **Standard mode**—One IPsec tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one IPsec tunnel that is established solely for it.
- **Aggregation mode**—One IPsec tunnel protects all data flows permitted by all the rules of an ACL. This mode is only used to communicate with old-version devices.
- **Per-host mode**—One IPsec tunnel protects one host-to-host data flow. One host-to-host data flow is identified by one ACL rule and protected by one IPsec tunnel established solely for it. This mode consumes more system resources when multiple data flows exist between two subnets to be protected.



## Application-based IPsec

Application-based IPsec does not require an ACL. You can implement application-based IPsec by one of the following methods:

- Bind an IPsec profile to an application protocol. All packets of the application protocol are encapsulated with IPsec. This method can be used to protect IPv6 routing protocols. The supported IPv6 routing protocols include OSPFv3, IPv6 BGP, and RIPng.
- Apply an IPsec profile to a tunnel interface. All packets routed to the tunnel interface are encapsulated with IPsec. This method can be used to protect only ADVPN tunnel packets.

All packets of the applications that are not bound to IPsec and the IPsec packets that failed to be de-encapsulated are dropped.

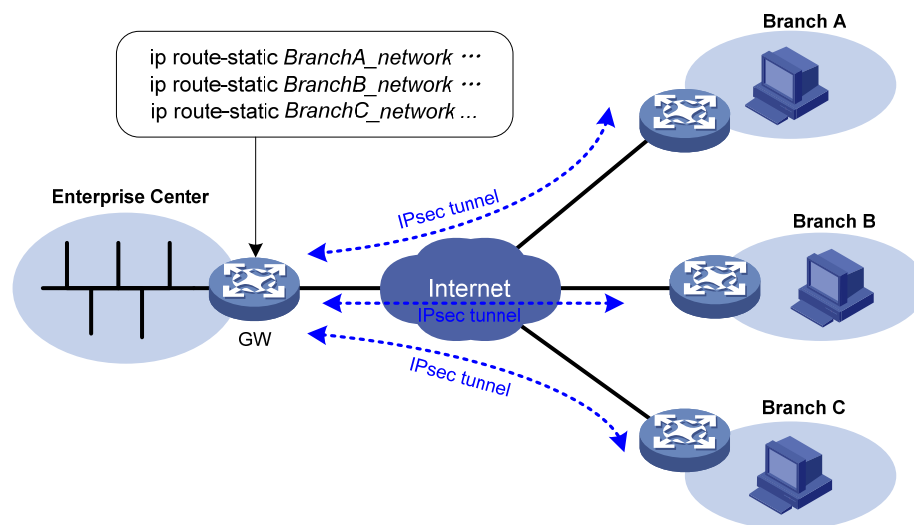
In one-to-many communication scenarios, you must configure the IPsec SAs for an IPv6 routing protocol in manual mode because of the following reasons:

- The automatic key exchange mechanism is used only to protect communications between two points. In one-to-many communication scenarios, automatic key exchange cannot be implemented.
- One-to-many communication scenarios require that all the devices use the same SA parameters (SPI and key) to receive and send packets. IKE negotiated SAs cannot meet this requirement.

## IPsec RRI

As shown in [Figure 99](#), the traffic between the enterprise center and the branches are protected by IPsec. The gateway at the enterprise center is configured with static routes to route traffic to the IPsec-protected interfaces. It is difficult to add or modify static routes on the gateway at the enterprise center if the IPsec VPN has a large number of branches or if the network structure changes.

**Figure 99 IPsec VPN**



IPsec Reverse Route Injection (RRI) enables an IPsec tunnel gateway to automatically add static routes destined for protected private networks or static routes destined for peer IPsec tunnel gateways to a routing table. As shown in [Figure 99](#), you can enable IPsec RRI on the gateway at the enterprise center. After an IPsec tunnel is established, the gateway automatically adds a static route to the routing table, which can be looked up. The destination IP address is the protected private network, and the next hop is the remote IP address of the IPsec tunnel. The traffic destined for the peer end is routed to the IPsec tunnel interface and thereby protected by IPsec.

You can advertise the static routes created by IPsec RRI in the internal network, and the internal network device can use them to forward traffic in the IPsec VPN.

In an MPLS L3VPN network, IPsec RRI can add static routes to VPN instances' routing tables.

IPsec RRI is applicable to gateways that must provide many IPsec tunnels (for example, a headquarters gateway).

## Protocols and standards

- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header*
- RFC 2406, *IP Encapsulating Security Payload*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*

## FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "[Configuring FIPS](#)") and non-FIPS mode.

## Security strength

By default, the device provides low encryption. To obtain high encryption, you must install the Strong Cryptography feature license. This feature provides stronger cryptography, additional IPsec tunnels, and higher encryption performance. For more information about obtaining the Strong Cryptography feature license, see the release notes or contact your Hewlett Packard Enterprise sales representative.

Support for features, commands, and parameters depends on the cryptography capability.

## IPsec tunnel establishment



### CAUTION:

Typically, IKE uses UDP port 500 for communication, and AH and ESP use the protocol numbers 51 and 50, respectively. Make sure traffic of these protocols is not denied on the interfaces with IKE or IPsec configured.

IPsec tunnels can be established in different methods. Choose a correct method to establish IPsec tunnels according to your network conditions:

- **ACL-based IPsec tunnel**—Protects packets identified by an ACL. To establish an ACL-based IPsec tunnel, configure an IPsec policy, specify an ACL in the policy, and apply the policy to an interface (see "[Implementing ACL-based IPsec](#)"). The IPsec tunnel establishment steps are the same in an IPv4 network and in an IPv6 network.
- **Application-based IPsec tunnel**—Protects the packets of an application. This method can be used to protect IPv6 routing protocols and ADVPN tunnels. It does not require an ACL. For information about IPv6 routing protocol protection, see "[Configuring IPsec for IPv6 routing protocols](#)." For information about ADVPN tunnel protection, see "[Configuring IPsec for tunnels](#)."

# Implementing ACL-based IPsec

Use the following procedure to implement ACL-based IPsec:

1. Configure an ACL for identifying data flows to be protected. To use IPsec to protect VPN traffic, you do not need to specify the VPN parameters in the ACL rules.
2. Configure IPsec transform sets to specify the security protocols, authentication and encryption algorithms, and the encapsulation mode.
3. Configure an IPsec policy to associate data flows with the IPsec transform sets, specify the SA negotiation mode, the peer IP addresses (the start and end points of the IPsec tunnel), the required keys, and the SA lifetime.

An IPsec policy is a set of IPsec policy entries that have the same name but different sequence numbers. In the same IPsec policy, an IPsec policy entry with a smaller sequence number has a higher priority.

4. Apply the IPsec policy to an interface.

Complete the following tasks to configure ACL-based IPsec:

| Tasks at a glance                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Required.) <a href="#">Configuring an ACL</a>                                                                                                                                                                                 |
| (Required.) <a href="#">Configuring an IPsec transform set</a>                                                                                                                                                                 |
| (Required.) Configure an IPsec policy (use either method): <ul style="list-style-type: none"><li>• <a href="#">Configuring a manual IPsec policy</a></li><li>• <a href="#">Configuring an IKE-based IPsec policy</a></li></ul> |
| (Required.) <a href="#">Applying an IPsec policy to an interface</a>                                                                                                                                                           |
| (Optional.) <a href="#">Enabling ACL checking for de-encapsulated packets</a>                                                                                                                                                  |
| (Optional.) <a href="#">Configuring IPsec anti-replay</a>                                                                                                                                                                      |
| (Optional.) <a href="#">Configuring IPsec anti-replay redundancy</a>                                                                                                                                                           |
| (Optional.) <a href="#">Binding a source interface to an IPsec policy</a>                                                                                                                                                      |
| (Optional.) <a href="#">Enabling QoS pre-classify</a>                                                                                                                                                                          |
| (Optional.) <a href="#">Enabling logging of IPsec packets</a>                                                                                                                                                                  |
| (Optional.) <a href="#">Configuring the DF bit of IPsec packets</a>                                                                                                                                                            |
| (Optional.) <a href="#">Configuring IPsec RRI</a>                                                                                                                                                                              |
| (Optional.) <a href="#">Configuring SNMP notifications for IPsec</a>                                                                                                                                                           |

## Configuring an ACL

IPsec uses ACLs to identify the traffic to be protected.

### Keywords in ACL rules

An ACL is a collection of ACL rules. Each ACL rule is a deny or permit statement. A permit statement identifies a data flow protected by IPsec, and a deny statement identifies a data flow that is not protected by IPsec. IPsec compares a packet against the ACL rules and processes the packet according to the first rule it matches.

- Each ACL rule matches both the outbound traffic and the returned inbound traffic. Suppose there is a rule **rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255**. This rule matches both traffic from 1.1.1.0 to 2.2.2.0 and traffic from 2.2.2.0 to 1.1.1.0.

- In the outbound direction, if a permit statement is matched, IPsec considers that the packet requires protection and continues to process it. If a deny statement is matched or no match is found, IPsec considers that the packet does not require protection and delivers it to the next function module.
- In the inbound direction:
  - Non-IPsec packets that match a permit statement are dropped.
  - IPsec packets destined for the device itself are de-encapsulated. By default, the de-encapsulated packets are compared against the ACL rules. Only those that match a permit statement are processed. Other packets are dropped. If ACL checking for de-encapsulated IPsec packets is disabled, the de-encapsulated packets are not compared against the ACL rules and are directly processed by other modules.

When defining ACL rules for IPsec, follow these guidelines:

- Permit only data flows that need to be protected and use the **any** keyword with caution. With the **any** keyword specified in a permit statement, all outbound traffic matching the permit statement will be protected by IPsec. All inbound IPsec packets matching the permit statement will be received and processed, but all inbound non-IPsec packets will be dropped. This will cause all the inbound traffic that does not need IPsec protection to be dropped.
- Avoid statement conflicts in the scope of IPsec policy entries. When creating a deny statement, be careful with its match scope and match order relative to permit statements. The policy entries in an IPsec policy have different match priorities. ACL rule conflicts between them are prone to cause mistreatment of packets. For example, when configuring a permit statement for an IPsec policy entry to protect an outbound traffic flow, you must avoid the situation that the traffic flow matches a deny statement in a higher priority IPsec policy entry. Otherwise, the packets will be sent out as normal packets. If they match a permit statement at the receiving end, they will be dropped by IPsec.

The following example shows how an improper statement causes unexpected packet dropping. Only the ACL-related configuration is presented.

Assume Router A is connected to subnet 1.1.2.0/24 and Router B is connected to subnet 3.3.3.0/24, and the IPsec policy configuration on Router A and Router B is as follows:

- IPsec configuration on Router A:
 

```

acl advanced 3000
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 deny ip
acl advanced 3001
 rule 0 permit ip source 1.1.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 1 deny ip
#
ipsec policy testa 1 isakmp <---IPsec policy entry with a higher priority
 security acl 3000
 ike-profile aa
 transform-set 1
#
ipsec policy testa 2 isakmp <---IPsec policy entry with a lower priority
 security acl 3001
 ike-profile bb
 transform-set 1

```
- IPsec configuration on Router B:
 

```

acl advanced 3001
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.2.0 0.0.0.255
 rule 1 deny ip

```

```
#
ipsec policy testb 1 isakmp
security acl 3001
ike-profile aa
transform-set 1
```

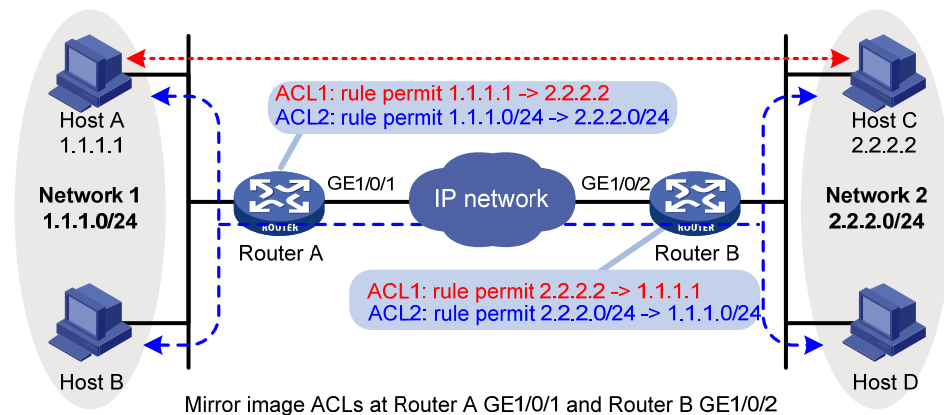
On Router A, apply the IPsec policy **testa** to the outbound interface of Router A. The IPsec policy contains two policy entries, **testa 1** and **testa 2**. The ACLs used by the two policy entries each contain a rule that matches traffic from 1.1.2.0/24 to 3.3.3.0/24. The one in policy entry **testa 1** is a deny statement and the one in policy entry **testa 2** is a permit statement. Because **testa 1** is matched prior to **testa 2**, traffic from 1.1.2.0/24 to 3.3.3.0/24 will match the deny statement and be sent as normal traffic. When the traffic arrives at Router B, the traffic matches rule 0 (a permit statement) in ACL 3001 in the applied IPsec policy **testb**. Because non-IPsec traffic that matches a permit statement must be dropped on the inbound interface, Router B drops the traffic.

To make sure subnet 1.1.2.0/24 can access subnet 3.3.3.0/24, you can delete the deny rule in ACL 3000 on Router A.

## Mirror image ACLs

To make sure SAs can be set up and the traffic protected by IPsec can be processed correctly between two IPsec peers, create mirror image ACLs on the IPsec peers. As shown in [Figure 100](#), ACL rules on Router B are mirror images of the rules on Router A. In this way, SAs can be created successfully for the traffic between Host A and Host C and for the traffic between Network 1 and Network 2.

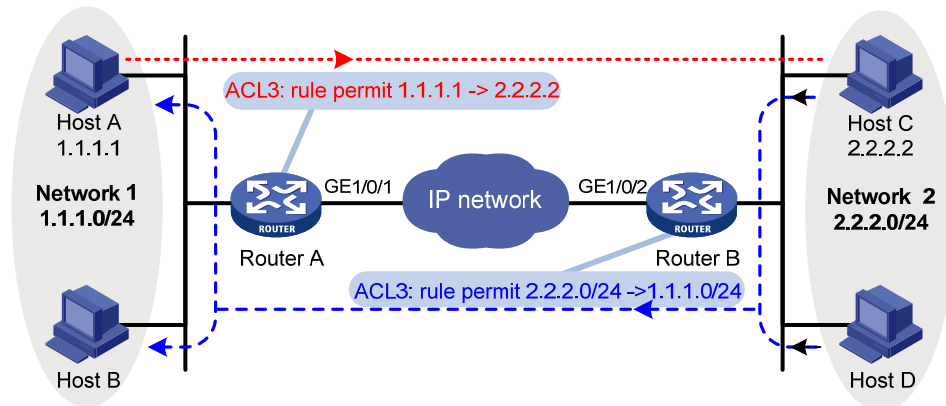
**Figure 100 Mirror image ACLs**



If the ACL rules on IPsec peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:

- The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer. As shown in [Figure 101](#), the range specified by the ACL rule configured on Router A is covered by its counterpart on Router B.
- The peer with the narrower rule initiates SA negotiation. If a wider ACL rule is used by the SA initiator, the negotiation request might be rejected because the matching traffic is beyond the scope of the responder. As shown in [Figure 101](#), the SA negotiation initiated by Host A to Host C is accepted but the SA negotiations from Host C to Host A, from Host C to Host B, and from Host D to Host A are rejected.

Figure 101 Non-mirror image ACLs



## Configuring an IPsec transform set

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, and authentication algorithms.

Changes to an IPsec transform set affect only SAs negotiated after the changes. To apply the changes to existing SAs, execute the **reset ipsec sa** command to clear the SAs so that they can be set up by using the updated parameters.

To configure an IPsec transform set:

| Step                                                          | Command                                                 | Remarks                                                                             |
|---------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                                      | N/A                                                                                 |
| 2. Create an IPsec transform set and enter its view.          | <b>ipsec transform-set</b><br><i>transform-set-name</i> | By default, no IPsec transform set exists.                                          |
| 3. Specify the security protocol for the IPsec transform set. | <b>protocol { ah   ah-esp   esp }</b>                   | Optional.<br>By default, the IPsec transform set uses ESP as the security protocol. |

| Step                                | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Specify the security algorithms. | <ul style="list-style-type: none"> <li>(Low encryption.) Specify the encryption algorithm for ESP:<br/><b>esp encryption-algorithm des-cbc</b></li> <li>(High encryption in non-FIPS mode.) Specify the encryption algorithm for ESP:<br/><b>esp encryption-algorithm { 3des-cbc   aes-cbc-128   aes-cbc-192   aes-cbc-256   aes-ctr-128   aes-ctr-192   aes-ctr-256   camellia-cbc-128   camellia-cbc-192   camellia-cbc-256   des-cbc   gmac-128   gmac-192   gmac-256   gcm-128   gcm-192   gcm-256   null   sm1-cbc-128   sm1-cbc-192   sm1-cbc-256   sm4-cbc } *</b></li> <li>(High encryption in FIPS mode.) Specify the encryption algorithm for ESP:<br/><b>esp encryption-algorithm { aes-cbc-128   aes-cbc-192   aes-cbc-256   aes-ctr-128   aes-ctr-192   aes-ctr-256   gmac-128   gmac-192   gmac-256   gcm-128   gcm-192   gcm-256 } *</b></li> <li>(In non-FIPS mode.) Specify the authentication algorithm for ESP:<br/><b>esp authentication-algorithm { aes-xcbc-mac   md5   sha1   sha256   sha384   sha512   sm3 } *</b></li> <li>(In FIPS mode.) Specify the authentication algorithm for ESP:<br/><b>esp authentication-algorithm { sha1   sha256   sha384   sha512 } *</b></li> <li>(In non-FIPS mode.) Specify the authentication algorithm for AH:<br/><b>ah authentication-algorithm { aes-xcbc-mac   md5   sha1   sha256   sha384   sha512   sm3 } *</b></li> <li>(In FIPS mode.) Specify the authentication algorithm for AH:<br/><b>ah authentication-algorithm { sha1   sha256   sha384   sha512 } *</b></li> </ul> | <p>Configure at least one command.</p> <p>By default, no security algorithm is specified.</p> <p>You can specify security algorithms for a security protocol only when the security protocol is used by the transform set. For example, you can specify the ESP-specific security algorithms only when you select ESP or AH-ESP as the security protocol.</p> <p>If you use ESP in FIPS mode, you must specify both the ESP encryption algorithm and the ESP authentication algorithm.</p> <p>You can specify multiple algorithms by using one command, and the algorithm specified earlier has a higher priority.</p> <p>The <b>aes-ctr-128</b>, <b>aes-ctr-192</b>, <b>aes-ctr-256</b>, <b>camellia-cbc-128</b>, <b>camellia-cbc-192</b>, <b>camellia-cbc-256</b>, <b>gmac-128</b>, <b>gmac-192</b>, <b>gmac-256</b>, <b>gcm-128</b>, <b>gcm-192</b>, and <b>gcm-256</b> encryption algorithms and the <b>aes-xcbc-mac</b>, <b>sha256</b>, <b>sha384</b>, and <b>sha512</b> authentication algorithms are available only for IKEv2.</p> |

| Step                                                                                  | Command                                                                                                                                                                                                                                                     | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Specify the mode in which the security protocol encapsulates IP packets.           | <b>encapsulation-mode { transport   tunnel }</b>                                                                                                                                                                                                            | <p>By default, the security protocol encapsulates IP packets in tunnel mode.</p> <p>The transport mode applies only when the source and destination IP addresses of data flows match those of the IPsec tunnel.</p> <p>IPsec for IPv6 routing protocols supports only the transport mode.</p> <p>IPsec for ADVPN tunnels supports only the tunnel mode.</p>                                                                                                        |
| 6. (Optional.) Enable the Perfect Forward Secrecy (PFS) feature for the IPsec policy. | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/><b>pfs { dh-group1   dh-group2   dh-group5   dh-group14   dh-group24   dh-group19   dh-group20 }</b></li> <li>In FIPS mode:<br/><b>pfs { dh-group14   dh-group19   dh-group20 }</b></li> </ul> | <p>By default, the PFS feature is not used for SA negotiation.</p> <p>For more information about PFS, see <a href="#">"Configuring IKE."</a></p> <p>The security level of the Diffie-Hellman (DH) group of the initiator must be higher than or equal to that of the responder.</p> <p>The end without the PFS feature performs SA negotiation according to the PFS requirements of the peer end.</p> <p>The DH groups 19 and 20 are available only for IKEv2.</p> |
| 7. (Optional.) Enable the Extended Sequence Number (ESN) feature.                     | <b>esn enable [ both ]</b>                                                                                                                                                                                                                                  | By default, the ESN feature is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Configuring a manual IPsec policy

In a manual IPsec policy, the parameters are configured manually, such as the keys, the SPIs, and the IP addresses of the two ends in tunnel mode.

### Configuration restrictions and guidelines

When you configure a manual IPsec policy, make sure the IPsec configuration at both ends of the IPsec tunnel meets the following requirements:

- The IPsec policies at the two ends must have IPsec transform sets that use the same security protocols, security algorithms, and encapsulation mode.
- The remote IPv4 address configured on the local end must be the same as the primary IPv4 address of the interface applied with the IPsec policy at the remote end. The remote IPv6 address configured on the local end must be the same as the first IPv6 address of the interface applied with the IPsec policy at the remote end.
- At each end, configure parameters for both the inbound SA and the outbound SA, and make sure the SAs in each direction are unique: For an outbound SA, make sure its triplet (remote IP address, security protocol, and SPI) is unique. For an inbound SA, make sure its SPI is unique.
- The local inbound SA must use the same SPI and keys as the remote outbound SA. The same is true of the local outbound SA and remote inbound SA.
- The keys for the local and remote inbound and outbound SAs must be in the same format. For example, if the local inbound SA uses a key in characters, the local outbound SA and remote inbound and outbound SAs must use keys in characters.



## Configuration procedure

To configure a manual IPsec policy:

| Step                                                         | Command                                                                                                                                                                                                                                                      | Remarks                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                        | <b>system-view</b>                                                                                                                                                                                                                                           | N/A                                                                                                                                                                                                                                                                                                                                  |
| 2. Create a manual IPsec policy entry and enter its view.    | <b>ipsec { ipv6-policy   policy }<br/>policy-name seq-number<br/>manual</b>                                                                                                                                                                                  | By default, no IPsec policy exists.                                                                                                                                                                                                                                                                                                  |
| 3. (Optional.) Configure a description for the IPsec policy. | <b>description text</b>                                                                                                                                                                                                                                      | By default, no description is configured.                                                                                                                                                                                                                                                                                            |
| 4. Specify an ACL for the IPsec policy.                      | <b>security acl [ ipv6 ] { acl-number<br/>  name acl-name }</b>                                                                                                                                                                                              | By default, no ACL is specified for an IPsec policy.<br>You can specify only one ACL for an IPsec policy.                                                                                                                                                                                                                            |
| 5. Specify an IPsec transform set for the IPsec policy.      | <b>transform-set<br/>transform-set-name</b>                                                                                                                                                                                                                  | By default, no IPsec transform set is specified for an IPsec policy.<br>You can specify only one IPsec transform set for a manual IPsec policy.                                                                                                                                                                                      |
| 6. Specify the remote IP address of the IPsec tunnel.        | <b>remote-address { ipv4-address  <br/>ipv6 ipv6-address }</b>                                                                                                                                                                                               | By default, the remote IP address of the IPsec tunnel is not specified.<br>The local IPv4 address of the IPsec tunnel is the primary IPv4 address of the interface to which the IPsec policy is applied. The local IPv6 address of the IPsec tunnel is the first IPv6 address of the interface to which the IPsec policy is applied. |
| 7. Configure an SPI for the inbound or outbound IPsec SA.    | <ul style="list-style-type: none"> <li>To configure an SPI for the inbound IPsec SA:<br/><b>sa spi inbound { ah   esp } spi-number</b></li> <li>To configure an SPI for the outbound IPsec SA:<br/><b>sa spi outbound { ah   esp } spi-number</b></li> </ul> | By default, no SPI is configured for the inbound or outbound IPsec SA.                                                                                                                                                                                                                                                               |

| Step                                | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. Configure keys for the IPsec SA. | <ul style="list-style-type: none"> <li>Configure an authentication key in hexadecimal format for AH:<br/><b>sa hex-key authentication { inbound   outbound } ah { cipher   simple } key-value</b></li> <li>Configure an authentication key in character format for AH:<br/><b>sa string-key { inbound   outbound } ah { cipher   simple } key-value</b></li> <li>Configure a key in character format for ESP:<br/><b>sa string-key { inbound   outbound } esp { cipher   simple } key-value</b></li> <li>Configure an authentication key in hexadecimal format for ESP:<br/><b>sa hex-key authentication { inbound   outbound } esp { cipher   simple } key-value</b></li> <li>Configure an encryption key in hexadecimal format for ESP:<br/><b>sa hex-key encryption { inbound   outbound } esp { cipher   simple } key-value</b></li> </ul> | <p>By default, no keys are configured for the IPsec SA.</p> <p>Configure keys correctly for the security protocol (AH, ESP, or both) you have specified in the IPsec transform set used by the IPsec policy.</p> <p>If you configure a key in both the character and the hexadecimal formats, only the most recent configuration takes effect.</p> <p>If you configure a key in character format for ESP, the device automatically generates an authentication key and an encryption key for ESP.</p> |

## Configuring an IKE-based IPsec policy

In an IKE-based IPsec policy, the parameters are automatically negotiated through IKE.

To configure an IKE-based IPsec policy, use one of the following methods:

- Directly configure it by configuring the parameters in IPsec policy view.
- Configure it by referencing an existing IPsec policy template with the parameters to be negotiated configured.

A device referencing an IPsec policy that is configured in this way cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. When the remote end's information (such as the IP address) is unknown, this method allows the remote end to initiate negotiations with the local end.

### Configuration restrictions and guidelines

When you configure an IKE-based IPsec policy, follow these restrictions and guidelines:

- The IPsec policies at the two tunnel ends must have IPsec transform sets that use the same security protocols, security algorithms, and encapsulation mode.
- The IPsec policies at the two tunnel ends must have the same IKE profile parameters.
- You can specify a maximum of six IPsec transform sets for an IKE-based IPsec policy. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.

- The remote IP address of the IPsec tunnel is required on an IKE negotiation initiator and is optional on the responder. The remote IP address specified on the local end must be the same as the local IP address specified on the remote end.
- The IPsec SA uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- The IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires.

### Directly configuring an IKE-based IPsec policy

| Step                                                          | Command                                                                                | Remarks                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                                                                     | N/A                                                                                                                                                                                                                                                                                                                                                                             |
| 2. Create an IKE-based IPsec policy entry and enter its view. | <b>ipsec { ipv6-policy   policy }</b><br><i>policy-name seq-number isakmp</i>          | By default, no IPsec policy exists.                                                                                                                                                                                                                                                                                                                                             |
| 3. (Optional.) Configure a description for the IPsec policy.  | <b>description</b> <i>text</i>                                                         | By default, no description is configured.                                                                                                                                                                                                                                                                                                                                       |
| 4. Specify an ACL for the IPsec policy.                       | <b>security acl [ ipv6 ] { acl-number   name acl-name } [ aggregation   per-host ]</b> | By default, no ACL is specified for an IPsec policy.<br>You can specify only one ACL for an IPsec policy.                                                                                                                                                                                                                                                                       |
| 5. Specify IPsec transform sets for the IPsec policy.         | <b>transform-set</b><br><i>transform-set-name&amp;&lt;1-6&gt;</i>                      | By default, no IPsec transform set is specified for an IPsec policy.                                                                                                                                                                                                                                                                                                            |
| 6. Specify an IKE profile for the IPsec policy.               | <b>ike-profile</b> <i>profile-name</i>                                                 | By default, no IKE profile is specified for an IPsec policy, and the device selects an IKE profile configured in system view for negotiation. If no IKE profile is configured, the globally configured IKE settings are used.<br>You can specify only one IKE profile for an IPsec policy.<br>For more information about IKE profiles, see " <a href="#">Configuring IKE</a> ." |
| 7. Specify an IKEv2 profile for the IPsec policy.             | <b>ikev2-profile</b> <i>profile-name</i>                                               | By default, no IKEv2 profile is specified for an IPsec policy.<br>You can specify only one IKEv2 profile for an IPsec policy.<br>For more information about IKEv2 profiles, see " <a href="#">Configuring IKEv2</a> ."                                                                                                                                                          |

| Step                                                                                                 | Command                                                                                                            | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. Specify the local IP address of the IPsec tunnel.                                                 | <b>local-address</b> { <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }                                     | By default, the local IPv4 address of IPsec tunnel is the primary IPv4 address of the interface to which the IPsec policy is applied, and the local IPv6 address of the IPsec tunnel is the first IPv6 address of the interface to which the IPsec policy is applied.<br><br>The local IP address specified by this command must be the same as the IP address used as the local IKE identity.<br><br>In a VRRP network, the local IP address must be the virtual IP address of the VRRP group to which the IPsec-applied interface belongs. |
| 9. Specify the remote IP address of the IPsec tunnel.                                                | <b>remote-address</b> { [ <b>ipv6</b> ] <i>host-name</i>   <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } | By default, the remote IP address of the IPsec tunnel is not specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 10. Set the IPsec SA lifetime.                                                                       | <b>sa duration</b> { <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> }                    | By default, the global SA lifetime is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 11. (Optional.) Set the IPsec SA idle timeout.                                                       | <b>sa idle-time</b> <i>seconds</i>                                                                                 | By default, the global SA idle timeout is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 12. (Optional.) Enables the Traffic Flow Confidentiality (TFC) padding feature.                      | <b>tfc enable</b>                                                                                                  | By default, the TFC padding feature is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 13. Return to system view.                                                                           | <b>quit</b>                                                                                                        | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 14. Set the global SA lifetime.                                                                      | <b>ipsec sa global-duration</b> { <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> }       | By default, the time-based SA lifetime is 3600 seconds, and the traffic-based SA lifetime is 1843200 kilobytes.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 15. (Optional.) Enable the global IPsec SA idle timeout feature, and set the global SA idle timeout. | <b>ipsec sa idle-time</b> <i>seconds</i>                                                                           | By default, the global IPsec SA idle timeout function is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Configuring an IKE-based IPsec policy by referencing an IPsec policy template

The configurable parameters for an IPsec policy template are the same as those when you directly configure an IKE-based IPsec policy. The difference is that more parameters are optional for an IPsec policy template. Except the IPsec transform sets and the IKE profile, all other parameters are optional.

A device referencing an IPsec policy that is configured by using an IPsec policy template cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. For example, in an IPsec policy template, the ACL is optional. If you do not specify an ACL, the IPsec protection range has no limit. So the device accepts all ACL settings of the negotiation initiator. When the remote end's information (such as the IP address) is unknown, the IPsec policy configured by using this method allows the remote end to initiate negotiations with the local end.

To configure an IKE-based IPsec policy by referencing an IPsec policy template:

| Step                                                                  | Command                                                                                | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                 | <b>system-view</b>                                                                     | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2. Create an IPsec policy template and enter its view.                | <b>ipsec { ipv6-policy-template   policy-template } template-name seq-number</b>       | By default, no IPsec policy template exists.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 3. (Optional.) Configure a description for the IPsec policy template. | <b>description text</b>                                                                | By default, no description is configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 4. (Optional.) Specify an ACL for the IPsec policy template.          | <b>security acl [ ipv6 ] { acl-number   name acl-name } [ aggregation   per-host ]</b> | By default, no ACL is specified for an IPsec policy template.<br>You can specify only one ACL for an IPsec policy template.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 5. Specify IPsec transform sets for the IPsec policy template.        | <b>transform-set transform-set-name&lt;1-6&gt;</b>                                     | By default, no IPsec transform set is specified for an IPsec policy template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 6. Specify an IKE profile for the IPsec policy template.              | <b>ike-profile profile-name</b>                                                        | By default, no IKE profile is specified for an IPsec policy template.<br><br>You can specify only one IKE profile for an IPsec policy template and the IKE profile cannot be used by another IPsec policy template or IPsec policy.<br><br>For more information about IKE profiles, see " <a href="#">Configuring IKE</a> ."                                                                                                                                                                                                                 |
| 7. Specify an IKEv2 profile for the IPsec policy template.            | <b>ikev2-profile profile-name</b>                                                      | By default, no IKEv2 profile is specified for an IPsec policy template.<br><br>You can specify only one IKEv2 profile for an IPsec policy template.<br><br>For more information about IKEv2 profiles, see " <a href="#">Configuring IKEv2</a> ."                                                                                                                                                                                                                                                                                             |
| 8. (Optional.) Specify the local IP address of the IPsec tunnel.      | <b>local-address { ipv4-address   ipv6 ipv6-address }</b>                              | By default, the local IPv4 address of IPsec tunnel is the primary IPv4 address of the interface to which the IPsec policy is applied, and the local IPv6 address of the IPsec tunnel is the first IPv6 address of the interface to which the IPsec policy is applied.<br><br>The local IP address specified by this command must be the same as the IP address used as the local IKE identity.<br><br>In a VRRP network, the local IP address must be the virtual IP address of the VRRP group to which the IPsec-applied interface belongs. |
| 9. (Optional.) Specify the remote IP address of the IPsec tunnel.     | <b>remote-address { [ ipv6 ] host-name   ipv4-address   ipv6 ipv6-address }</b>        | By default, the remote IP address of the IPsec tunnel is not specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Step                                                                                                 | Command                                                                                                                              | Remarks                                                                                                 |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 10. Configure the IPsec SA lifetime.                                                                 | <b>sa duration</b> { <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> }                                      | By default, the global SA lifetime settings are used.                                                   |
| 11. (Optional.) Set the IPsec SA idle timeout.                                                       | <b>sa idle-time</b> <i>seconds</i>                                                                                                   | By default, the global SA idle timeout is used.                                                         |
| 12. (Optional.) Enables the Traffic Flow Confidentiality (TFC) padding feature.                      | <b>tfc enable</b>                                                                                                                    | By default, the TFC padding feature is disabled.                                                        |
| 13. Return to system view.                                                                           | <b>quit</b>                                                                                                                          | N/A                                                                                                     |
| 14. Configure the global SA lifetime.                                                                | <b>ipsec sa global-duration</b> { <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> }                         | By default, time-based SA lifetime is 3600 seconds, and traffic-based SA lifetime is 1843200 kilobytes. |
| 15. (Optional.) Enable the global IPsec SA idle timeout feature, and set the global SA idle timeout. | <b>ipsec sa idle-time</b> <i>seconds</i>                                                                                             | By default, the global IPsec SA idle timeout function is disabled.                                      |
| 16. Create an IPsec policy by referencing the IPsec policy template.                                 | <b>ipsec</b> { <b>ipv6-policy</b>   <b>policy</b> } <i>policy-name seq-number</i> <b>isakmp</b> <b>template</b> <i>template-name</i> | By default, no IPsec policy exists.                                                                     |

## Applying an IPsec policy to an interface

You can apply an IPsec policy to an interface to protect certain data flows. To cancel the IPsec protection, remove the application of the IPsec policy. In addition to physical interfaces, such as serial and Ethernet interfaces, you can apply an IPsec policy to virtual interfaces, such as tunnel and virtual template interfaces, to protect applications such as GRE and L2TP.

For each packet to be sent out of an interface applied with an IPsec policy, the interface looks through the IPsec policy entries in the IPsec policy in ascending order of sequence numbers. If the packet matches the ACL of an IPsec policy entry, the interface uses the IPsec policy entry to protect the packet. If no match is found, the interface sends the packet out without IPsec protection.

When the interface receives an IPsec packet whose destination address is the IP address of the local device, it searches for the inbound IPsec SA according to the SPI carried in the IPsec packet header for de-encapsulation. If the de-encapsulated packet matches the permit rule of the ACL, the device processes the packet. Otherwise, it drops the packet.

To apply an IPsec policy to an interface:

| Step                     | Command                                                        | Remarks |
|--------------------------|----------------------------------------------------------------|---------|
| 1. Enter system view.    | <b>system-view</b>                                             | N/A     |
| 2. Enter interface view. | <b>interface</b> <i>interface-type</i> <i>interface-number</i> | N/A     |

| Step                                                                                                                                       | Command                                                                      | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Apply an IPsec policy to the interface.                                                                                                 | <b>ipsec apply</b> { <b>policy</b>   <b>ipv6-policy</b> } <i>policy-name</i> | By default, no IPsec policy is applied to the interface.<br>You can apply only one IPsec policy to an interface.<br>An IKE-based IPsec policy can be applied to multiple interfaces, and a manual IPsec policy can be applied to only one interface.                                                                                                                                                                                                                                                                   |
| 4. Specify a traffic processing card or device for the interface (distributed devices in standalone mode/centralized devices in IRF mode). | <b>service slot</b> <i>slot-number</i>                                       | By default, no traffic processing card or device is specified.<br>It is required when the following conditions are met: <ul style="list-style-type: none"> <li>An IKE-based IPsec policy is applied to global logical interfaces, such as VLAN interfaces and tunnel interfaces.</li> <li>The IPsec anti-replay function is globally enabled.</li> </ul> The traffic processing card or device specified for a tunnel interface must be the card or device where the source interface of the tunnel interface resides. |
| 5. Specify a traffic processing card for the interface (distributed devices in IRF mode).                                                  | <b>service chassis</b> <i>chassis-number slot slot-number</i>                | By default, no traffic processing card is specified.<br>It is required when the following conditions are met: <ul style="list-style-type: none"> <li>An IKE-based IPsec policy is applied to global logical interfaces, such as VLAN interfaces and tunnel interfaces.</li> <li>The IPsec anti-replay function is globally enabled.</li> </ul> The traffic processing card specified for a tunnel interface must be the card where the source interface of the tunnel interface resides.                               |

## Enabling ACL checking for de-encapsulated packets

This feature compares the de-encapsulated incoming IPsec packets against the ACL in the IPsec policy and discards those that do not match the ACL. This feature can protect networks against attacks using forged IPsec packets.

This feature applies only to tunnel-mode IPsec.

To enable ACL checking for de-encapsulated packets:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                                | Command                           | Remarks                              |
|-----------------------------------------------------|-----------------------------------|--------------------------------------|
| 2. Enable ACL checking for de-encapsulated packets. | <b>ipsec decrypt-check enable</b> | By default, this feature is enabled. |

## Configuring IPsec anti-replay

IPsec anti-replay protects networks against anti-replay attacks by using a sliding window mechanism called anti-replay window. This feature checks the sequence number of each received IPsec packet against the current IPsec packet sequence number range of the sliding window. If the sequence number is not in the current sequence number range, the packet is considered a replayed packet and is discarded.

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets is not required, and the de-encapsulation process consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay can check and discard replayed packets before de-encapsulation.

In some situations, service data packets are received in a different order than their original order. The IPsec anti-replay function drops them as replayed packets, which impacts communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

IPsec anti-replay does not affect manually created IPsec SAs. According to the IPsec protocol, only IKE-based IPsec SAs support anti-replay checking.

### ⓘ IMPORTANT:

- IPsec anti-replay is enabled by default. Failure to detect anti-replay attacks might result in denial of services. Use caution when you disable IPsec anti-replay.
- Set the anti-replay window size as small as possible to reduce the impact on system performance.
- Typically, a distributed device processes packets for a global logical interface directly on the service cards that received the packets. However, IPsec anti-replay requires that packets sent and received on the same global logical interface be processed by the same service card. To implement IPsec anti-replay on distributed devices, use the **service** command in the global logical interface view to specify a service card for forwarding the traffic on the interface.

To configure IPsec anti-replay:

| Step                                             | Command                                      | Remarks                                   |
|--------------------------------------------------|----------------------------------------------|-------------------------------------------|
| 1. Enter system view.                            | <b>system-view</b>                           | N/A                                       |
| 2. Enable IPsec anti-replay.                     | <b>ipsec anti-replay check</b>               | By default, IPsec anti-replay is enabled. |
| 3. Set the size of the IPsec anti-replay window. | <b>ipsec anti-replay window <i>width</i></b> | The default size is 64.                   |

## Configuring IPsec anti-replay redundancy

This feature synchronizes the following information from the active device to the standby device at configurable packet-based intervals:

- Lower bound values of the IPsec anti-replay window for inbound packets.
- IPsec anti-replay sequence numbers for outbound packets.

This feature, used together with IPsec redundancy, ensures uninterrupted IPsec traffic forwarding and anti-replay protection when the active device fails.



To configure IPsec anti-replay redundancy:

| Step                                                                                                                                              | Command                                                                                                                                                                                                                                                                                                                          | Remarks                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                                                                                             | <b>system-view</b>                                                                                                                                                                                                                                                                                                               | N/A                                                                                                                                                               |
| 2. Enable IPsec redundancy.                                                                                                                       | <b>ipsec redundancy enable</b>                                                                                                                                                                                                                                                                                                   | By default, IPsec redundancy is disabled.                                                                                                                         |
| 3. Enter IPsec policy view or IPsec policy template view.                                                                                         | <ul style="list-style-type: none"> <li>Enter IPsec policy view:<br/><b>ipsec { policy   ipv6-policy }</b><br/><i>policy-name seq-number</i><br/><b>[ isakmp   manual ]</b></li> <li>Enter IPsec policy template view:<br/><b>ipsec { policy-template   ipv6-policy-template }</b><br/><i>template-name seq-number</i></li> </ul> | N/A                                                                                                                                                               |
| 4. Set the anti-replay window synchronization interval for inbound packets and the sequence number synchronization interval for outbound packets. | <b>redundancy replay-interval</b><br><b>inbound</b> <i>inbound-interval</i><br><b>outbound</b> <i>outbound-interval</i>                                                                                                                                                                                                          | By default, the active device synchronizes the anti-replay window every time it receives 1000 packets and the sequence number every time it sends 100000 packets. |

## Binding a source interface to an IPsec policy

For high availability, a core device is usually connected to an ISP through two links, which operate in backup or load sharing mode. The two interfaces negotiate with their peers to establish IPsec SAs respectively. When one interface fails and a link failover occurs, the other interface needs to take some time to renegotiate SAs, resulting in service interruption.

To solve these problems, bind a source interface to an IPsec policy and apply the policy to both interfaces. This enables the two physical interfaces to use the same source interface to negotiate IPsec SAs. As long as the source interface is up, the negotiated IPsec SAs will not be removed and will keep working, regardless of link failover.

Follow these guidelines when you perform this task:

- Only the IKE-based IPsec policies can be bound to a source interface.
- An IPsec policy can be bound to only one source interface.
- A source interface can be bound to multiple IPsec policies.
- If the source interface bound to an IPsec policy is removed, the IPsec policy becomes a common IPsec policy.
- If no local address is specified for an IPsec policy that has been bound to a source interface, the IPsec policy uses the IP address of the bound source interface to perform IKE negotiation. If a local address is specified, the IPsec policy uses the local address to perform IKE negotiation.

To bind a source interface to an IPsec policy:

| Step                                           | Command                                                                                                             | Remarks                                                      |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 1. Enter system view.                          | <b>system-view</b>                                                                                                  | N/A                                                          |
| 2. Bind a source interface to an IPsec policy. | <b>ipsec { ipv6-policy   policy }</b><br><i>policy-name local-address</i><br><i>interface-type interface-number</i> | By default, no source interface is bound to an IPsec policy. |

## Enabling QoS pre-classify

### ⚠ CAUTION:

If you configure both IPsec and QoS on an interface, make sure the IPsec traffic classification rules match the QoS traffic classification rules. If the rules do not match, QoS might classify the packets of one IPsec SA to different queues, causing packets to be sent out of order. When IPsec anti-replay is enabled, IPsec will drop the incoming packets that are out of the anti-replay window, resulting in packet loss.

If you apply both an IPsec policy and a QoS policy to an interface, QoS classifies packets by using the new headers added by IPsec. If you want QoS to classify packets by using the headers of the original IP packets, enable the QoS pre-classify feature.

IPsec traffic classification rules are determined by the specified ACL rules. For more information about QoS policy and classification, see *ACL and QoS Configuration Guide*.

To enable the QoS pre-classify feature:

| Step                                                      | Command                                                                                                                                                                                                                                                                                                            | Remarks                                   |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 1. Enter system view.                                     | <b>system-view</b>                                                                                                                                                                                                                                                                                                 | N/A                                       |
| 2. Enter IPsec policy view or IPsec policy template view. | <ul style="list-style-type: none"><li>To enter IPsec policy view:<br/><b>ipsec { policy   ipv6-policy }<br/>policy-name seq-number<br/>[ isakmp   manual ]</b></li><li>To enter IPsec policy template view:<br/><b>ipsec { policy-template  <br/>ipv6-policy-template }<br/>template-name seq-number</b></li></ul> | N/A                                       |
| 3. Enable QoS pre-classify.                               | <b>qos pre-classify</b>                                                                                                                                                                                                                                                                                            | By default, QoS pre-classify is disabled. |

## Enabling logging of IPsec packets

Perform this task to enable the logging of IPsec packets that are discarded because of reasons such as IPsec SA lookup failure, AH-ESP authentication failure, and ESP encryption failure. The log information includes the source and destination IP addresses, SPI value, and sequence number of a discarded IPsec packet, and the reason for the discard.

To enable the logging of IPsec packets:

| Step                                    | Command                            | Remarks                                               |
|-----------------------------------------|------------------------------------|-------------------------------------------------------|
| 1. Enter system view.                   | <b>system-view</b>                 | N/A                                                   |
| 2. Enable the logging of IPsec packets. | <b>ipsec logging packet enable</b> | By default, the logging of IPsec packets is disabled. |

## Configuring the DF bit of IPsec packets

Perform this task to configure the Don't Fragment (DF) bit in the new IP header of IPsec packets in one of the following ways:

- **clear**—Clears the DF bit in the new header.
- **set**—Sets the DF bit in the new header.

- **copy**—Copies the DF bit in the original IP header to the new IP header.

You can configure the DF bit in system view and interface view. The interface-view DF bit setting takes precedence over the system-view DF bit setting. If the interface-view DF bit setting is not configured, the interface uses the system-view DF bit setting.

Follow these guidelines when you configure the DF bit:

- The DF bit setting takes effect only in tunnel mode, and it changes the DF bit in the new IP header rather than the original IP header.
- Configure the same DF bit setting on the interfaces where the same IPsec policy bound to a source interface has been applied.
- If the DF bit is set, the devices on the path cannot fragment the IPsec packets. Therefore, make sure the path MTU is larger than the IPsec packets. Otherwise, the IPsec packets will be discarded. If the path MTU is smaller than the IPsec packets, clear the DF bit.

To configure the DF bit of IPsec packets on an interface:

| Step                                                       | Command                                                           | Remarks                                                   |
|------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------|
| 1. Enter system view.                                      | <b>system-view</b>                                                | N/A                                                       |
| 2. Enter interface view.                                   | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                                       |
| 3. Configure the DF bit of IPsec packets on the interface. | <b>ipsec df-bit { clear   copy   set }</b>                        | By default, the interface uses the global DF bit setting. |

To configure the DF bit of IPsec packets globally:

| Step                                               | Command                                           | Remarks                                                                             |
|----------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------|
| 1. Enter system view.                              | <b>system-view</b>                                | N/A                                                                                 |
| 2. Configure the DF bit of IPsec packets globally. | <b>ipsec global-df-bit { clear   copy   set }</b> | By default, IPsec copies the DF bit in the original IP header to the new IP header. |

## Configuring IPsec RRI

### Configuration guidelines

When you enable or disable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs created by this IPsec policy, and the associated static routes.

If you change the preference value or tag value for an IPsec policy, the device deletes all IPsec SAs created by this IPsec policy, and the associated static routes. Your change takes effect for future IPsec RRI-created static routes.

You can set preferences for the static routes created by IPsec RRI to flexibly apply route management policies. For example, you can set the same preference for multiple routes to the same destination to implement load sharing, or you can set different preferences to implement route backup.

You can also set tags for the static routes created by IPsec RRI to implement flexible route control through routing policies.

IPsec RRI does not generate a static route to a destination address to be protected if the destination address is not defined in the ACL that an IPsec policy or an IPsec policy template uses. You must manually configure a static route to the destination address.

## Configuration procedure

To configure IPsec RRI:

| Step                                                                               | Command                                                                                                                                                                                                                                                                               | Remarks                                                                                              |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                              | <b>system-view</b>                                                                                                                                                                                                                                                                    | N/A                                                                                                  |
| 2. Enter IPsec policy view or IPsec policy template view.                          | <ul style="list-style-type: none"><li>To enter IPsec policy view:<br/><b>ipsec { policy   ipv6-policy } policy-name seq-number isakmp</b></li><li>To enter IPsec policy template view:<br/><b>ipsec { policy-template   ipv6-policy-template } template-name seq-number</b></li></ul> | N/A                                                                                                  |
| 3. Enable IPsec RRI.                                                               | <b>reverse-route dynamic</b>                                                                                                                                                                                                                                                          | By default, IPsec RRI is disabled.<br>IPsec RRI is supported in both tunnel mode and transport mode. |
| 4. Optional.) Set the preference value for the static routes created by IPsec RRI. | <b>reverse-route preference</b> <i>number</i>                                                                                                                                                                                                                                         | The default value is 60.                                                                             |
| 5. (Optional.) Set the tag value for the static routes created by IPsec RRI.       | <b>reverse-route tag</b> <i>tag-value</i>                                                                                                                                                                                                                                             | The default value is 0.                                                                              |

# Configuring IPsec for IPv6 routing protocols

## Configuration task list

Complete the following tasks to configure IPsec for IPv6 routing protocols:

| Tasks at a glance                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------|
| (Required.) <a href="#">Configuring an IPsec transform set</a>                                                          |
| (Required.) <a href="#">Configuring a manual IPsec profile</a>                                                          |
| (Required.) Applying the IPsec profile to an IPv6 routing protocol (see <i>Layer 3—IP Routing Configuration Guide</i> ) |
| (Optional.) <a href="#">Enabling logging of IPsec packets</a>                                                           |
| (Optional.) <a href="#">Configuring SNMP notifications for IPsec</a>                                                    |

## Configuring a manual IPsec profile

A manual IPsec profile is similar to a manual IPsec policy. The difference is that an IPsec profile is uniquely identified by a name and it does not support ACL configuration. A manual IPsec profile specifies the IPsec transform set used for protecting data flows, and the SPIs and keys used by the SAs.

When you configure a manual IPsec profile, make sure the IPsec profile configuration at both tunnel ends meets the following requirements:

- The IPsec transform set used by the IPsec profile at the two tunnel ends must have the same security protocol, encryption and authentication algorithms, and packet encapsulation mode.
- The local inbound and outbound IPsec SAs must have the same SPI and key.
- The IPsec SAs on the devices in the same scope must have the same key. The scope is defined by protocols. For OSPF, the scope consists of OSPF neighbors or an OSPF area. For RIPng, the scope consists of directly-connected neighbors or a RIPng process. For BGP, the scope consists of BGP peers or a BGP peer group.
- The keys for the IPsec SAs at the two tunnel ends must be configured in the same format. For example, if the key at one end is entered as a string of characters, the key on the other end must also be entered as a string of characters.

To configure a manual IPsec profile:

| Step                                                          | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2. Create a manual IPsec profile and enter its view.          | <b>ipsec profile</b> <i>profile-name</i> <b>manual</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | By default, no IPsec profile exists. The <b>manual</b> keyword is not needed if you enter the view of an existing IPsec profile.                                                                                                                                                                                                                                                                                                     |
| 3. (Optional.) Configure a description for the IPsec profile. | <b>description</b> <i>text</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | By default, no description is configured.                                                                                                                                                                                                                                                                                                                                                                                            |
| 4. Specify an IPsec transform set.                            | <b>transform-set</b> <i>transform-set-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | By default, no IPsec transform set is specified for an IPsec profile. The specified IPsec transform set must use the transport mode.                                                                                                                                                                                                                                                                                                 |
| 5. Configure an SPI for an SA.                                | <b>sa spi</b> { <b>inbound</b>   <b>outbound</b> } { <b>ah</b>   <b>esp</b> } <i>spi-number</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | By default, no SPI is configured for an SA.                                                                                                                                                                                                                                                                                                                                                                                          |
| 6. Configure keys for the IPsec SA.                           | <ul style="list-style-type: none"> <li>• Configure an authentication key in hexadecimal format for AH:<br/><b>sa hex-key authentication</b> { <b>inbound</b>   <b>outbound</b> } <b>ah</b> { <b>cipher</b>   <b>simple</b> } <i>key-value</i></li> <li>• Configure an authentication key in character format for AH:<br/><b>sa string-key</b> { <b>inbound</b>   <b>outbound</b> } <b>ah</b> { <b>cipher</b>   <b>simple</b> } <i>key-value</i></li> <li>• Configure a key in character format for ESP:<br/><b>sa string-key</b> { <b>inbound</b>   <b>outbound</b> } <b>esp</b> [ <b>cipher</b>   <b>simple</b> ] <i>key-value</i></li> <li>• Configure an authentication key in hexadecimal format for ESP:<br/><b>sa hex-key authentication</b> { <b>inbound</b>   <b>outbound</b> } <b>esp</b> { <b>cipher</b>   <b>simple</b> } <i>key-value</i></li> <li>• Configure an encryption key in hexadecimal format for ESP:<br/><b>sa hex-key encryption</b> { <b>inbound</b>   <b>outbound</b> } <b>esp</b> { <b>cipher</b>   <b>simple</b> } <i>key-value</i></li> </ul> | <p>By default, no keys are configured for the IPsec SA.</p> <p>Configure a key for the security protocol (AH, ESP, or both) you have specified.</p> <p>If you configure a key in character format for ESP, the device automatically generates an authentication key and an encryption key for ESP.</p> <p>If you configure a key in both the character and hexadecimal formats, only the most recent configuration takes effect.</p> |

# Configuring IPsec for tunnels

## Configuration task list

Complete the following tasks to configure IPsec for tunnels:

| Tasks at a glance                                                                     |
|---------------------------------------------------------------------------------------|
| (Required.) <a href="#">Configuring an IPsec transform set</a>                        |
| (Required.) <a href="#">Configuring an IKE-based IPsec profile</a>                    |
| (Required.) <a href="#">Applying an IKE-based IPsec profile to a tunnel interface</a> |
| (Optional.) <a href="#">Enabling logging of IPsec packets</a>                         |
| (Optional.) <a href="#">Configuring SNMP notifications for IPsec</a>                  |

## Configuring an IKE-based IPsec profile

An IKE-based IPsec profile is similar to an IKE-based IPsec policy. The difference is that an IPsec profile is uniquely identified by a name and it does not support ACL configuration. An IKE-based IPsec profile specifies the IPsec transform sets used for protecting data flows, and the IKE profile used for IKE negotiation.

When you configure an IKE-based IPsec profile, follow these restrictions and guidelines:

- The IPsec profiles at the two tunnel ends must have IPsec transform sets that use the same security protocols, security algorithms, and encapsulation mode.
- The IPsec profiles at the two tunnel ends must have the same IKE profile parameters.
- You can specify a maximum of six IPsec transform sets for an IKE-based IPsec profile. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.
- The IPsec SA uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- The IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires.

To configure an IKE-based IPsec profile:

| Step                                                          | Command                                         | Remarks                                                                                                                          |
|---------------------------------------------------------------|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                              | N/A                                                                                                                              |
| 2. Create an IKE-based IPsec profile and enter its view.      | <b>ipsec profile <i>profile-name</i> isakmp</b> | By default, no IPsec profile exists. The <b>isakmp</b> keyword is not needed if you enter the view of an existing IPsec profile. |
| 3. (Optional.) Configure a description for the IPsec profile. | <b>description <i>text</i></b>                  | By default, no description is configured.                                                                                        |

| Step                                                                                                | Command                                                                                                         | Remarks                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Specify IPsec transform sets.                                                                    | <b>transform-set</b><br><i>transform-set-name</i> &<1-6>                                                        | By default, no IPsec transform set is specified for an IPsec profile.<br>The specified IPsec transform sets must use the tunnel mode.                                                                                                                                                                                                                                                            |
| 5. Specify an IKE profile.                                                                          | <b>ike-profile</b> <i>profile-name</i>                                                                          | By default, no IKE profile is specified for an IPsec profile, and the device selects an IKE profile configured in system view for negotiation. If no IKE profile is configured in system view, the globally configured IKE settings are used.<br>You can specify only one IKE profile for an IPsec profile.<br>For more information about IKE profiles, see " <a href="#">Configuring IKE</a> ." |
| 6. Set the IPsec SA lifetime.                                                                       | <b>sa duration</b> { <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> }                 | By default, the global SA lifetime is used.                                                                                                                                                                                                                                                                                                                                                      |
| 7. (Optional.) Set the IPsec SA idle timeout.                                                       | <b>sa idle-time</b> <i>seconds</i>                                                                              | By default, the global SA idle timeout is used.                                                                                                                                                                                                                                                                                                                                                  |
| 8. Set the global SA lifetime.                                                                      | <b>ipsec sa global-duration</b><br>{ <b>time-based</b> <i>seconds</i>   <b>traffic-based</b> <i>kilobytes</i> } | By default, the time-based SA lifetime is 3600 seconds, and the traffic-based SA lifetime is 1843200 kilobytes.                                                                                                                                                                                                                                                                                  |
| 9. (Optional.) Enable the global IPsec SA idle timeout feature, and set the global SA idle timeout. | <b>ipsec sa idle-time</b> <i>seconds</i>                                                                        | By default, the global IPsec SA idle timeout function is disabled.                                                                                                                                                                                                                                                                                                                               |

## Applying an IKE-based IPsec profile to a tunnel interface

After an IKE-based IPsec profile is applied to a tunnel interface, the peers negotiate an IPsec tunnel through IKE to protect data transmitted through the tunnel interface.

IKE-based IPsec profiles can be applied only to ADVPN tunnel interfaces.

To apply an IKE-based IPsec profile to a tunnel interface:

| Step                                                                 | Command                                                                                             | Remarks                                                          |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                  | N/A                                                              |
| 2. Create an ADVPN tunnel interface and enter tunnel interface view. | <b>interface tunnel</b> <i>number</i> <b>mode advpn</b> { <b>gre</b>   <b>udp</b> } [ <b>ipv6</b> ] | By default, no tunnel interface exists on the device.            |
| 3. Apply an IKE-based IPsec profile to the tunnel interface.         | <b>tunnel protection ipsec profile</b> <i>profile-name</i>                                          | By default, no IPsec profile is applied to the tunnel interface. |

## Configuring SNMP notifications for IPsec

After you enable SNMP notifications for IPsec, the IPsec module notifies the NMS of important module events. The notifications are sent to the device's SNMP module. You can configure the notification transmission parameters for the SNMP module to specify how the SNMP module

displays notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To generate and output SNMP notifications for a specific IPsec failure or event type, perform the following tasks:

1. Enable SNMP notifications for IPsec globally.
2. Enable SNMP notifications for the failure or event type.

To configure SNMP notifications for IPsec:

| Step                                                                   | Command                                                                                                                                                                                                                                                                                                   | Remarks                                                                      |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 1. Enter system view                                                   | <b>system-view</b>                                                                                                                                                                                                                                                                                        | N/A                                                                          |
| 2. Enable SNMP notifications for IPsec globally.                       | <b>snmp-agent trap enable ipsec global</b>                                                                                                                                                                                                                                                                | By default, SNMP notifications for IPsec are disabled.                       |
| 3. Enable SNMP notifications for the specified failure or event types. | <b>snmp-agent trap enable ipsec</b><br>[ <b>auth-failure</b>   <b>decrypt-failure</b>   <b>encrypt-failure</b>   <b>invalid-sa-failure</b>   <b>no-sa-failure</b>   <b>policy-add</b>   <b>policy-attach</b>   <b>policy-delete</b>   <b>policy-detach</b>   <b>tunnel-start</b>   <b>tunnel-stop</b> ] * | By default, SNMP notifications for all failure and event types are disabled. |

## Displaying and maintaining IPsec

Execute **display** commands in any view and **reset** commands in user view.

| Task                                       | Command                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display IPsec policy information.          | <b>display ipsec</b> { <b>ipv6-policy</b>   <b>policy</b> } [ <i>policy-name</i> [ <i>seq-number</i> ] ]                                                                                                                                                                                                                                     |
| Display IPsec policy template information. | <b>display ipsec</b> { <b>ipv6-policy-template</b>   <b>policy-template</b> } [ <i>template-name</i> [ <i>seq-number</i> ] ]                                                                                                                                                                                                                 |
| Display IPsec profile information.         | <b>display ipsec profile</b> [ <i>profile-name</i> ]                                                                                                                                                                                                                                                                                         |
| Display IPsec transform set information.   | <b>display ipsec transform-set</b> [ <i>transform-set-name</i> ]                                                                                                                                                                                                                                                                             |
| Display IPsec SA information.              | <b>display ipsec sa</b> [ <b>brief</b>   <b>count</b>   <b>interface</b> <i>interface-type interface-number</i>   { <b>ipv6-policy</b>   <b>policy</b> } <i>policy-name</i> [ <i>seq-number</i> ]   <b>profile</b> <i>policy-name</i>   <b>remote</b> [ <b>ipv6</b> ] <i>ip-address</i> ]                                                    |
| Display IPsec statistics.                  | <b>display ipsec statistics</b> [ <b>tunnel-id</b> <i>tunnel-id</i> ]                                                                                                                                                                                                                                                                        |
| Display IPsec tunnel information.          | <b>display ipsec tunnel</b> { <b>brief</b>   <b>count</b>   <b>tunnel-id</b> <i>tunnel-id</i> }                                                                                                                                                                                                                                              |
| Clear IPsec SAs.                           | <b>reset ipsec sa</b> [ { { <b>ipv6-policy</b>   <b>policy</b> } <i>policy-name</i> [ <i>seq-number</i> ]   <b>profile</b> <i>policy-name</i>   <b>remote</b> { <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }   <b>spi</b> { <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } } { <b>ah</b>   <b>esp</b> } <i>spi-num</i> ] |
| Clear IPsec statistics.                    | <b>reset ipsec statistics</b> [ <b>tunnel-id</b> <i>tunnel-id</i> ]                                                                                                                                                                                                                                                                          |



# IPsec configuration examples

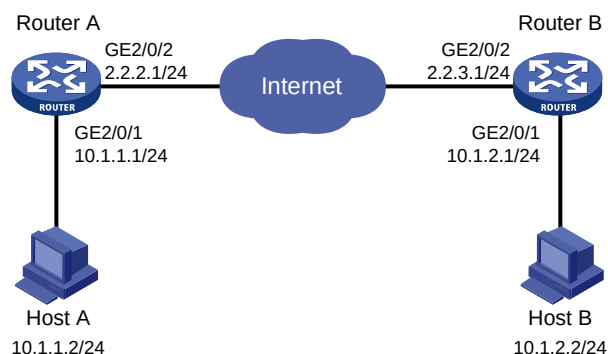
## Configuring a manual mode IPsec tunnel for IPv4 packets

### Network requirements

As shown in [Figure 102](#), establish an IPsec tunnel between Router A and Router B to protect data flows between subnet 10.1.1.0/24 and subnet 10.1.2.0/24. Configure the tunnel as follows:

- Specify the encapsulation mode as tunnel, the security protocol as ESP, the encryption algorithm as 128-bit AES, and the authentication algorithm as HMAC-SHA1.
- Manually set up IPsec SAs.

**Figure 102 Network diagram**



### Configuration procedure

1. Configure Router A:
  - # Configure IP addresses for interfaces. (Details not shown.)
  - # Configure an ACL to identify data flows from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.
  - ```
<RouterA> system-view
[RouterA] acl advanced 3101
[RouterA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[RouterA-acl-ipv4-adv-3101] quit
```
 - # Configure a static route to Host B. The command uses the direct next hop address (2.2.2.3) as an example.
 - ```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 gigabitethernet 2/0/2 2.2.2.3
```
  - # Create an IPsec transform set named **tran1**.
  - ```
[RouterA] ipsec transform-set tran1
```
 - # Specify the encapsulation mode as **tunnel**.
 - ```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
  - # Specify the security protocol as **ESP**.
  - ```
[RouterA-ipsec-transform-set-tran1] protocol esp
```
 - # Specify the ESP encryption and authentication algorithms.
 - ```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```
  - # Create a manual IPsec policy entry with the name **map1** and the sequence number 10.
  - ```
[RouterA] ipsec policy map1 10 manual
```

```

# Apply ACL 3101.
[RouterA-ipsec-policy-manual-map1-10] security acl 3101
# Apply the IPsec transform set tran1.
[RouterA-ipsec-policy-manual-map1-10] transform-set tran1
# Specify the remote IP address of the IPsec tunnel as 2.2.3.1.
[RouterA-ipsec-policy-manual-map1-10] remote-address 2.2.3.1
# Configure inbound and outbound SPIs for ESP.
[RouterA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[RouterA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
# Configure the inbound and outbound SA keys for ESP.
[RouterA-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
[RouterA-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
[RouterA-ipsec-policy-manual-map1-10] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 2/0/2.
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] ip address 2.2.2.1 255.255.255.0
[RouterA-GigabitEthernet2/0/2] ipsec apply policy map1
[RouterA-GigabitEthernet2/0/2] quit

```

2. Configure Router B:

```

# Configure IP addresses for interfaces. (Details not shown.)
# Configure an ACL to identify data flows from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<RouterB> system-view
[RouterB] acl advanced 3101
[RouterB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[RouterB-acl-ipv4-adv-3101] quit
# Configure a static route to Host A. The command uses the direct next hop address (2.2.3.3)
as an example.
[RouterB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/0/2 2.2.3.3
# Create an IPsec transform set named tran1.
[RouterB] ipsec transform-set tran1
# Specify the encapsulation mode as tunnel.
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[RouterB-ipsec-transform-set-tran1] protocol esp
# Specify the ESP encryption and authentication algorithms.
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
# Create a manual IPsec policy entry with the name use1 and the sequence number 10.
[RouterB] ipsec policy use1 10 manual
# Apply ACL 3101.
[RouterB-ipsec-policy-manual-use1-10] security acl 3101
# Apply IPsec transform set tran1.
[RouterB-ipsec-policy-manual-use1-10] transform-set tran1
# Specify the remote IP address of the IPsec tunnel as 2.2.2.1.
[RouterB-ipsec-policy-manual-use1-10] remote-address 2.2.2.1

```

```
# Configure the inbound and outbound SPIs for ESP.
[RouterB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[RouterB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
# Configure the inbound and outbound SA keys for ESP.
[RouterB-ipsec-policy-manual-use1-10] sa string-key outbound esp simple gfedcba
[RouterB-ipsec-policy-manual-use1-10] sa string-key inbound esp simple abcdefg
[RouterB-ipsec-policy-manual-use1-10] quit
# Apply the IPsec policy use1 to interface GigabitEthernet 2/0/2.
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ipsec policy use1
[RouterB-GigabitEthernet2/0/2] quit
```

Verifying the configuration

After the configuration is completed, an IPsec tunnel between Router A and Router B is established, and the traffic between subnet 10.1.1.0/24 and subnet 10.1.2.0/24 is IPsec protected. This example uses Router A to verify the configuration.

Use the **display ipsec sa** command to display IPsec SAs on Router A.

```
[RouterA] display ipsec sa
-----
Interface: GigabitEthernet2/0/2
-----

-----
IPsec policy: map1
Sequence number: 10
Mode: Manual
-----

Tunnel id: 549
Encapsulation mode: tunnel
Path MTU: 1443
Tunnel:
    local address: 2.2.2.1
    remote address: 2.2.3.1
Flow:
    as defined in ACL 3101
[Inbound ESP SA]
    SPI: 54321 (0x0000d431)
    Connection ID: 1
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    No duration limit for this SA
[Outbound ESP SA]
    SPI: 12345 (0x00003039)
    Connection ID: 2
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    No duration limit for this SA
```

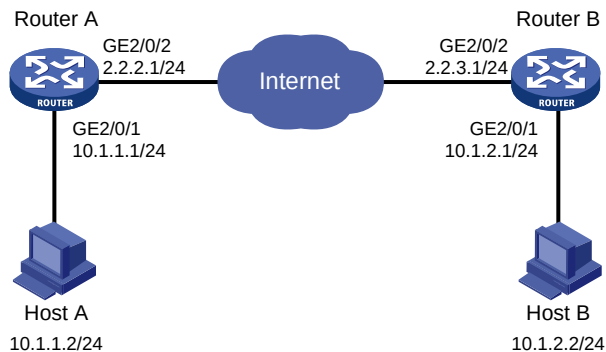
Configuring an IKE-based IPsec tunnel for IPv4 packets

Network requirements

As shown in [Figure 103](#), establish an IPsec tunnel between Router A and Router B to protect data flows between subnet 10.1.1.0/24 and subnet 10.1.2.0/24. Configure the IPsec tunnel as follows:

- Specify the encapsulation mode as tunnel, the security protocol as ESP, the encryption algorithm as 128-bit AES, and the authentication algorithm as HMAC-SHA1.
- Set up SAs through IKE negotiation.

Figure 103 Network diagram



Configuration procedure

1. Configure Router A:

Configure IP addresses for interfaces. (Details not shown.)

Configure an ACL to identify data flows from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<RouterA> system-view
```

```
[RouterA] acl advanced 3101
```

```
[RouterA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[RouterA-acl-ipv4-adv-3101] quit
```

Configure a static route to Host B. The command uses the direct next hop address (2.2.2.3) as an example.

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 gigabitethernet 2/0/2 2.2.2.3
```

Create an IPsec transform set named **tran1**.

```
[RouterA] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[RouterA-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption and authentication algorithms.

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

```
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[RouterA-ipsec-transform-set-tran1] quit
```

Create and configure the IKE keychain named **keychain1**.

```
[RouterA] ike keychain keychain1
```

Specify the plaintext **123456TESTplat&!** as the pre-shared key to be used with the remote peer at 2.2.3.1.

```

[RouterA-ike-keychain-keychain1] pre-shared-key address 2.2.3.1 255.255.255.0 key
simple 123456TESTplat&!
[RouterA-ike-keychain-keychain1] quit
# Create and configure the IKE profile named profile1.
[RouterA] ike profile profile1
[RouterA-ike-profile-profile1] keychain keychain1
[RouterA-ike-profile-profile1] match remote identity address 2.2.3.1 255.255.255.0
[RouterA-ike-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
[RouterA] ipsec policy map1 10 isakmp
# Apply ACL 3101.
[RouterA-ipsec-policy-isakmp-map1-10] security acl 3101
# Apply the IPsec transform set tran1.
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
# Specify the local and remote IP addresses of the IPsec tunnel as 2.2.2.1 and 2.2.3.1.
[RouterA-ipsec-policy-isakmp-map1-10] local-address 2.2.2.1
[RouterA-ipsec-policy-isakmp-map1-10] remote-address 2.2.3.1
# Apply the IKE profile profile1.
[RouterA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[RouterA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 2/0/2.
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] ip address 2.2.2.1 255.255.255.0
[RouterA-GigabitEthernet2/0/2] ipsec apply policy map1
[RouterA-GigabitEthernet2/0/2] quit

```

2. Configure Router B:

```

# Configure IP addresses for interfaces. (Details not shown.)
# Configure an ACL to identify data flows from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<RouterB> system-view
[RouterB] acl advanced 3101
[RouterB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[RouterB-acl-ipv4-adv-3101] quit
# Configure a static route to Host A. The command uses the direct next hop address (2.2.3.3)
as an example.
[RouterB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/0/2 2.2.3.3
# Create an IPsec transform set named tran1.
[RouterB] ipsec transform-set tran1
# Specify the encapsulation mode as tunnel.
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[RouterB-ipsec-transform-set-tran1] protocol esp
# Specify the ESP encryption and authentication algorithms.
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
# Create and configure the IKE keychain named keychain1.

```

```

[RouterB] ike keychain keychain1
[RouterB-ike-keychain-keychain1] pre-shared-key address 2.2.2.1 255.255.255.0 key
simple 123456TESTplat&!
[RouterB-ike-keychain-keychain1] quit
# Create and configure the IKE profile named profile1.
[RouterB] ike profile profile1
[RouterB-ike-profile-profile1] keychain keychain1
[RouterB-ike-profile-profile1] match remote identity address 2.2.2.1 255.255.255.0
[RouterB-ike-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 10.
[RouterB] ipsec policy use1 10 isakmp
# Apply ACL 3101.
[RouterB-ipsec-policy-isakmp-use1-10] security acl 3101
# Apply the IPsec transform set tran1.
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
# Specify the local and remote IP addresses of the IPsec tunnel as 2.2.3.1 and 2.2.2.1.
[RouterB-ipsec-policy-isakmp-use1-10] local-address 2.2.3.1
[RouterB-ipsec-policy-isakmp-use1-10] remote-address 2.2.2.1
# Apply the IKE profile profile1.
[RouterB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[RouterB-ipsec-policy-isakmp-use1-10] quit
# Apply the IPsec policy use1 to interface GigabitEthernet 2/0/2.
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ip address 2.2.3.1 255.255.255.0
[RouterB-GigabitEthernet2/0/2] ipsec apply policy use1
[RouterB-GigabitEthernet2/0/2] quit

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, the traffic between the two subnets is IPsec protected.

Use the **display ipsec sa** command to display IPsec SAs on Router A and Router B. This example uses Router A to verify the configuration.

```

[RouterA] display ipsec sa
-----
Interface: GigabitEthernet2/0/2
-----

-----
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Path MTU: 1443
Tunnel:
    local address: 2.2.3.1

```

```

remote address: 2.2.2.1
Flow:
sour addr: 2.2.3.1/0.0.0.0  port: 0  protocol: ip
dest addr: 2.2.2.1/0.0.0.0  port: 0  protocol: ip

[Inbound ESP SAs]
SPI: 3769702703 (0xe0b1192f)
Connection ID: 1
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 3000/28800
SA remaining duration (kilobytes/sec): 2300/797
Max received sequence-number: 1
Anti-replay check enable: N
Anti-replay window size:
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3840956402 (0xe4f057f2)
Connection ID: 2
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 3000/28800
SA remaining duration (kilobytes/sec): 2312/797
Max sent sequence-number: 1
UDP encapsulation used for NAT traversal: N
Status: Active

```

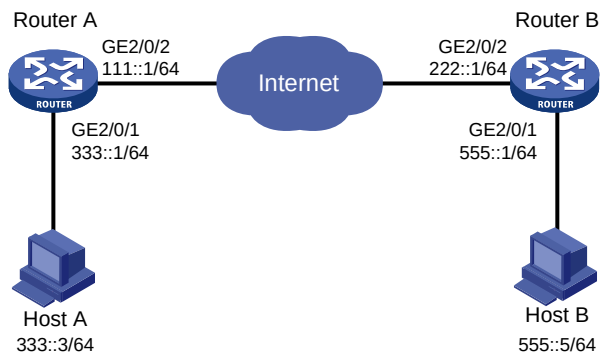
Configuring an IKE-based IPsec tunnel for IPv6 packets

Network requirements

As shown in [Figure 104](#), establish an IPsec tunnel between Router A and Router B to protect data flows between subnet 333::/64 and subnet 555::/64. Configure the IPsec tunnel as follows:

- Specify the encapsulation mode as tunnel, the security protocol as ESP, the encryption algorithm as 128-bit AES, and the authentication algorithm as HMAC-SHA1.
- Set up SAs through IKE negotiation.

Figure 104 Network diagram



Configuration procedure

1. Configure Router A:

Configure IPv6 addresses for interfaces. (Details not shown.)

Configure an ACL to identify data flows from subnet 333::/64 to subnet 555::/64.

```
<RouterA> system-view
```

```
[RouterA] acl ipv6 advanced 3101
```

```
[RouterA-acl-ipv6-adv-3101] rule permit ipv6 source 333::0 64 destination 555::0 64
```

```
[RouterA-acl-ipv6-adv-3101] quit
```

Configure a static route to Host B. The command uses the direct next hop address (111::2) as an example.

```
[RouterA] ipv6 route-static 555::0 64 111::2
```

Create an IPsec transform set named **tran1**.

```
[RouterA] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[RouterA-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption and authentication algorithms.

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

```
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[RouterA-ipsec-transform-set-tran1] quit
```

Create and configure the IKE keychain named **keychain1**.

```
[RouterA] ike keychain keychain1
```

```
[RouterA-ike-keychain-keychain1] pre-shared-key address ipv6 222::1 64 key simple  
123456TESTplat&!
```

```
[RouterA-ike-keychain-keychain1] quit
```

Create and configure the IKE profile named **profile1**.

```
[RouterA] ike profile profile1
```

```
[RouterA-ike-profile-profile1] keychain keychain1
```

```
[RouterA-ike-profile-profile1] match remote identity address ipv6 222::1 64
```

```
[RouterA-ike-profile-profile1] quit
```

Create an IKE-based IPsec policy entry with the name **map1** and the sequence number 10.

```
[RouterA] ipsec ipv6-policy map1 10 isakmp
```

Apply IPv6 ACL 3101.

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] security acl ipv6 3101
```

Apply the IPsec transform set **tran1**.

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] transform-set tran1
```

Specify the local and remote IPv6 addresses of the IPsec tunnel as 111::1 and 222::1.

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] local-address ipv6 111::1
```

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] remote-address ipv6 222::1
```

Apply the IKE profile **profile1**.

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] ike-profile profile1
```

```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] quit
```

Apply the IPsec policy **map1** to interface GigabitEthernet 2/0/2.

```
[RouterA] interface gigabitethernet 2/0/2
```

```
[RouterA-GigabitEthernet2/0/2] ipv6 address 111::1/64
```

```
[RouterA-GigabitEthernet2/0/2] ipsec apply ipv6-policy map1
```



```

[RouterA-GigabitEthernet2/0/2] quit
2. Configure Router B:
# Configure IPv6 addresses for interfaces. (Details not shown.)
# Configure an ACL to identify data flows from subnet 555::/64 to subnet 333::/64.
<RouterB> system-view
[RouterB] acl ipv6 advanced 3101
[RouterB-acl-ipv6-adv-3101] rule permit ipv6 source 555::/64 destination 333::/64
[RouterB-acl-ipv6-adv-3101] quit
# Configure a static route to Host A. The command uses the direct next hop address (222::2) as
an example.
[RouterB] ipv6 route-static 333::0 64 222::2
# Create an IPsec transform set named tran1.
[RouterB] ipsec transform-set tran1
# Specify the encapsulation mode as tunnel.
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[RouterB-ipsec-transform-set-tran1] protocol esp
# Specify the ESP encryption and authentication algorithms.
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
# Create and configure the IKE keychain named keychain1.
[RouterB] ike keychain keychain1
[RouterB-ike-keychain-keychain1] pre-shared-key address ipv6 111::1 64 key simple
123456TESTplat&!
[RouterB-ike-keychain-keychain1] quit
# Create and configure the IKE profile named profile1.
[RouterB] ike profile profile1
[RouterB-ike-profile-profile1] keychain keychain1
[RouterB-ike-profile-profile1] match remote identity address ipv6 111::1 64
[RouterB-ike-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 10.
[RouterB] ipsec ipv6-policy use1 10 isakmp
# Apply ACL 3101.
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] security acl ipv6 3101
# Apply the IPsec transform set tran1.
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] transform-set tran1
# Specify the local and remote IPv6 addresses of the IPsec tunnel as 222::1 and 111::1.
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] local-address ipv6 222::1
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] remote-address ipv6 111::1
# Apply the IKE profile profile1.
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] ike-profile profile1
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] quit
# Apply the IPsec policy use1 to interface GigabitEthernet 2/0/2.
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ipv6 address 222::1/64
[RouterB-GigabitEthernet2/0/2] ipsec apply ipv6-policy use1

```

```
[RouterB-GigabitEthernet2/0/2] quit
```

Verifying the configuration

Initiate a connection from subnet 333::/64 to subnet 555::/64 to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, the traffic between the two subnets is IPsec protected.

Use the **display ipsec sa** command to display IPsec SAs on Router A and Router B. This example uses Router A to verify the configuration.

```
[RouterA] display ipsec sa
```

```
-----  
Interface: GigabitEthernet2/0/2  
-----
```

```
-----  
IPsec policy: map1
```

```
Sequence number: 10
```

```
Mode: ISAKMP  
-----
```

```
Tunnel id: 0
```

```
Encapsulation mode: tunnel
```

```
Perfect Forward Secrecy:
```

```
Path MTU: 1423
```

```
Tunnel:
```

```
    local  address: 111::1
```

```
    remote address: 222::1
```

```
Flow:
```

```
sour addr: 111::1/0      port: 0  protocol: ipv6
```

```
dest addr: 222::1/0      port: 0  protocol: ipv6
```

```
[Inbound ESP SAs]
```

```
  SPI: 3769702703 (0xe0b1192f)
```

```
  Connection ID: 1
```

```
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
```

```
  SA duration (kilobytes/sec): 3000/28800
```

```
  SA remaining duration (kilobytes/sec): 2300/797
```

```
  Max received sequence-number: 1
```

```
  Anti-replay check enable: N
```

```
  Anti-replay window size:
```

```
  UDP encapsulation used for NAT traversal: N
```

```
  Status: Active
```

```
[Outbound ESP SAs]
```

```
  SPI: 3840956402 (0xe4f057f2)
```

```
  Connection ID: 2
```

```
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
```

```
  SA duration (kilobytes/sec): 3000/28800
```

```
  SA remaining duration (kilobytes/sec): 2312/797
```

```
  Max sent sequence-number: 1
```

```
  UDP encapsulation used for NAT traversal: N
```

```
  Status: Active
```

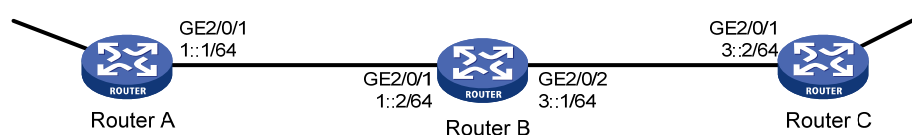
Configuring IPsec for RIPng

Network requirements

As shown in [Figure 105](#), Router A, Router B, and Router C learn IPv6 routes through RIPng.

Establish an IPsec tunnel between the routers to protect the RIPng packets transmitted in between. Specify the security protocol as ESP, the encryption algorithm as 128-bit AES, and the authentication algorithm as HMAC-SHA1 for the IPsec tunnel.

Figure 105 Network diagram



Requirements analysis

To meet the network requirements, perform the following tasks:

1. Configure basic RIPng.
For more information about RIPng configuration, see *Layer 3—IP Routing Configuration Guide*.
2. Configure an IPsec profile.
 - The IPsec profiles on all the routers must have IPsec transform sets that use the same security protocol, authentication and encryption algorithms, and encapsulation mode.
 - The SPI and key configured for the inbound SA and those for the outbound SA must be the same on each router.
 - The SPI and key configured for the SAs on all the routers must be the same.
3. Apply the IPsec profile to a RIPng process or to an interface.

Configuration procedure

1. Configure Router A:
Configure IPv6 addresses for interfaces. (Details not shown.)
Configure basic RIPng.

```
<RouterA> system-view
[RouterA] ripng 1
[RouterA-ripng-1] quit
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ripng 1 enable
[RouterA-GigabitEthernet2/0/1] quit
```


Create and configure the IPsec transform set named **tran1**.

```
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterA-ipsec-transform-set-tran1] protocol esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```


Create and configure the IPsec profile named **profile001**.

```
[RouterA] ipsec profile profile001 manual
[RouterA-ipsec-profile-profile001] transform-set tran1
[RouterA-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterA-ipsec-profile-profile001] sa spi inbound esp 123456
```

```
[RouterA-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterA-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterA-ipsec-profile-profile001] quit
# Apply the IPsec profile to RIPng process 1.
[RouterA] ripng 1
[RouterA-ripng-1] enable ipsec-profile profile001
[RouterA-ripng-1] quit
```

2. Configure Router B:

Configure IPv6 addresses for interfaces. (Details not shown.)

Configure basic RIPng.

```
<RouterB> system-view
[RouterB] ripng 1
[RouterB-ripng-1] quit
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ripng 1 enable
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ripng 1 enable
[RouterB-GigabitEthernet2/0/2] quit
```

Create and configure the IPsec transform set named **tran1**.

```
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterB-ipsec-transform-set-tran1] protocol esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

Create and configure the IPsec profile named **profile001**.

```
[RouterB] ipsec profile profile001 manual
[RouterB-ipsec-profile-profile001] transform-set tran1
[RouterB-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterB-ipsec-profile-profile001] sa spi inbound esp 123456
[RouterB-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterB-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterB-ipsec-profile-profile001] quit
```

Apply the IPsec profile to RIPng process 1.

```
[RouterB] ripng 1
[RouterB-ripng-1] enable ipsec-profile profile001
[RouterB-ripng-1] quit
```

3. Configure Router C:

Configure IPv6 addresses for interfaces. (Details not shown.)

Configure basic RIPng.

```
<RouterC> system-view
[RouterC] ripng 1
[RouterC-ripng-1] quit
[RouterC] interface gigabitethernet 2/0/1
[RouterC-GigabitEthernet2/0/1] ripng 1 enable
[RouterC-GigabitEthernet2/0/1] quit
```

```

# Create and configure the IPsec transform set named tran1.
[RouterC] ipsec transform-set tran1
[RouterC-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterC-ipsec-transform-set-tran1] protocol esp
[RouterC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterC-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterC-ipsec-transform-set-tran1] quit

# Create and configure the IPsec profile named profile001.
[RouterC] ipsec profile profile001 manual
[RouterC-ipsec-profile-profile001] transform-set tran1
[RouterC-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterC-ipsec-profile-profile001] sa spi inbound esp 123456
[RouterC-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterC-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterC-ipsec-profile-profile001] quit

# Apply the IPsec profile to RIPng process 1.
[RouterC] ripng 1
[RouterC-ripng-1] enable ipsec-profile profile001
[RouterC-ripng-1] quit

```

Verifying the configuration

After the configuration is completed, Router A, Router B, and Router C learn IPv6 routing information through RIPng. IPsec SAs are set up successfully on the routers to protect RIPng packets. This example uses Router A to verify the configuration.

Use the **display ripng** command to display the RIPng configuration. The output shows that the IPsec profile **profile001** has been applied to RIPng process 1.

```

[RouterA] display ripng 1
  RIPng process : 1
    Preference : 100
    Checkzero : Enabled
    Default Cost : 0
    Maximum number of balanced paths : 8
    Update time : 30 sec(s) Timeout time : 180 sec(s)
    Suppress time : 120 sec(s) Garbage-Collect time : 120 sec(s)
    Number of periodic updates sent : 186
    Number of trigger updates sent : 1
    IPsec profile name: profile001

```

Use the **display ipsec sa** command to display the established IPsec SAs.

```

[RouterA] display ipsec sa
-----
Global IPsec SA
-----

-----
IPsec profile: profile001
Mode: Manual
-----

Encapsulation mode: transport

```

```

[Inbound ESP SA]
  SPI: 123456 (0x3039)
  Connection ID: 1
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  No duration limit for this SA

[Outbound ESP SA]
  SPI: 123456 (0x3039)
  Connection ID: 2
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  No duration limit for this SA

```

Configuring IPsec RRI

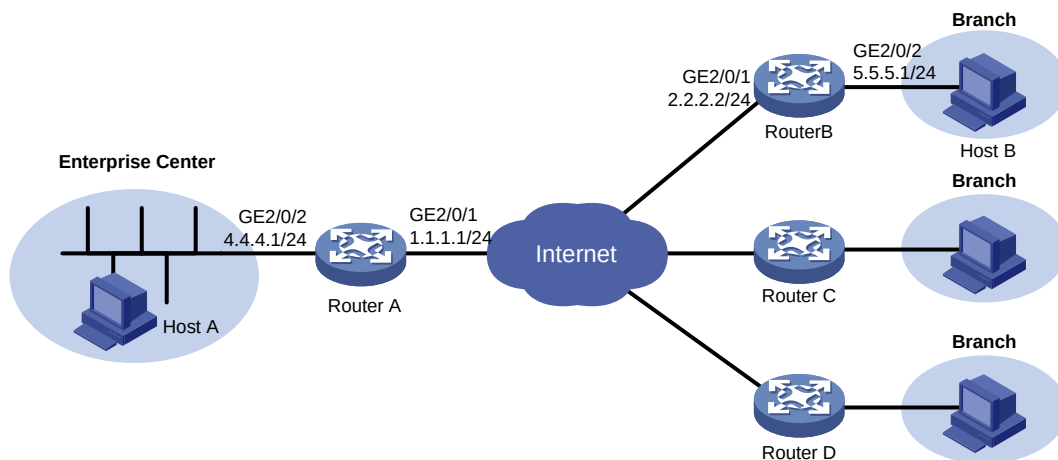
Network requirements

As shown in [Figure 106](#), branches access the enterprise center through an IPsec VPN.

Configure the IPsec VPN as follows:

- Configure an IPsec tunnel between Router A and each branch gateway (Router B, Router C, and Router D) to protect traffic between subnets 4.4.4.0/24 and 5.5.5.0/24.
- Configure the tunnels to use the security protocol **ESP**, the encryption algorithm **DES**, and the authentication algorithm **SHA1-HMAC-96**. Use IKE for IPsec SA negotiation.
- Configure IKE proposal to use pre-shared key authentication method, the encryption algorithm 3DES, and the authentication algorithm **HMAC-SHA1**.
- Configure IPsec RRI on Router A to automatically create static routes to the branches based on the established IPsec SAs.

Figure 106 Network diagram



Configuration procedure

1. Assign IPv4 addresses to the interfaces on the routers according to [Figure 106](#). (Details not shown.)
2. Configure Router A:


```

# Create an IPsec transform set named tran1, and specify ESP as the security protocol, DES
as the encryption algorithm, and HMAC-SHA-1-96 as the authentication algorithm.
<RouterA> system-view
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel

```

```

[RouterA-ipsec-transform-set-tran1] protocol esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
# Create an IPsec policy template named temp1, referencing the transform set tran1.
[RouterA] ipsec policy-template temp1 1
[RouterA-ipsec-policy-template-temp1-1] transform-set tran1
# Enable IPsec RRI, set the preference to 100 and the tag to 1000 for the static routes created
by IPsec RRI.
[RouterA-ipsec-policy-template-temp1-1] reverse-route dynamic
[RouterA-ipsec-policy-template-temp1-1] reverse-route preference 100
[RouterA-ipsec-policy-template-temp1-1] reverse-route tag 1000
[RouterA-ipsec-policy-template-temp1-1] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10 by
referencing IPsec policy template temp1.
[RouterA] ipsec policy map1 10 isakmp template temp1
# Create an IKE proposal named 1, and specify 3DES as the encryption algorithm,
HMAC-SHA1 as the authentication algorithm, and pre-share as the authentication method.
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterA-ike-proposal-1] authentication-algorithm sha
[RouterA-ike-proposal-1] authentication-method pre-share
[RouterA-ike-proposal-1] quit
# Create an IKE keychain named key1 and specify the plaintext 123 as the pre-shared key to
be used with the remote peer at 2.2.2.2.
[RouterA] ike keychain key1
[RouterA-ike-keychain-key1] pre-shared-key address 2.2.2.2 key simple 123
[RouterA-ike-keychain-key1] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 2/0/1.
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ipsec apply policy map1
[RouterA-GigabitEthernet2/0/1] quit

```

3. Configure Router B:

```

# Create an IPsec transform set named tran1, and specify ESP as the security protocol, DES
as the encryption algorithm, and HMAC-SHA-1-96 as the authentication algorithm.
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
[RouterB-ipsec-transform-set-tran1] protocol esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
# Configure ACL 3000 to identify traffic from subnet 5.5.5.0/24 to subnet 4.4.4.0/24.
[RouterB] acl advanced 3000
[RouterB-acl-ipv4-adv-3000] rule permit ip source 5.5.5.0 0.0.0.255 destination
4.4.4.0 0.0.0.255
[RouterB-acl-ipv4-adv-3000] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
Specify the transform set tran1 and ACL 3000, and specify the remote IP address for the tunnel
as 1.1.1.1.

```

```

[RouterB] ipsec policy map1 10 isakmp
[RouterB-ipsec-policy-isakmp-map1-10] transform-set tran1
[RouterB-ipsec-policy-isakmp-map1-10] security acl 3000
[RouterB-ipsec-policy-isakmp-map1-10] remote-address 1.1.1.1
[RouterB-ipsec-policy-isakmp-map1-10] quit
# Create an IKE proposal named 1, and specify 3DES as the encryption algorithm,
HMAC-SHA1 as the authentication algorithm, and pre-share as the authentication method.
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterB-ike-proposal-1] authentication-algorithm sha
[RouterB-ike-proposal-1] authentication-method pre-share
[RouterB-ike-proposal-1] quit
# Create an IKE keychain named key1 and specify the plaintext 123 as the pre-shared key to
be used with the remote peer at 1.1.1.1.
[RouterB] ike keychain key1
[RouterB-ike-keychain-key1] pre-shared-key address 1.1.1.1 key simple 123
[RouterB-ike-keychain-key1] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ipsec apply policy map1
[RouterB-GigabitEthernet2/0/1] quit
Make sure Router B has a route to the peer private network, with the outgoing interface as
GigabitEthernet 2/0/1.

```

4. Configure Router C and Router D in the same way Router B is configured.

Verifying the configuration

1. Verify that IPsec RRI can automatically create a static route from Router A to Router B:


```

# Initiate a connection from subnet 5.5.5.0/24 to subnet 4.4.4.0/24. IKE negotiation is triggered
to establish IPsec SAs between Router A and Router B. (Details not shown.)
# Verify that IPsec SAs are established on Router A.
[RouterA] display ipsec sa
-----
Interface: GigabitEthernet2/0/1
-----

-----
IPsec policy: map1
Sequence number: 10
Mode: Template
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1463
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2
Flow:
sour addr: 4.4.4.0/255.255.255.0 port: 0 protocol: ip

```


dest addr: 5.5.5.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 1014286405 (0x3c74c845)
Connection ID: 1
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3590
Max received sequence-number: 4
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for nat traversal: N
Status: Active

[Outbound ESP SAs]

SPI: 4011716027 (0xef1dedbb)
Connection ID: 2
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3590
Max sent sequence-number: 4
UDP encapsulation used for nat traversal: N
Status: Active

Verify that IPsec RRI has created a static route to reach Router B.

[RouterA] display ip routing-table verbose

2. Verify that Router A can automatically create static routes to Router C and Router D in the same way that you verify the IPsec RRI function by using Router A and Router B. (Details not shown.)

Configuring IKE

Unless otherwise specified, the term "IKE" in this chapter refers to IKEv1.

Overview

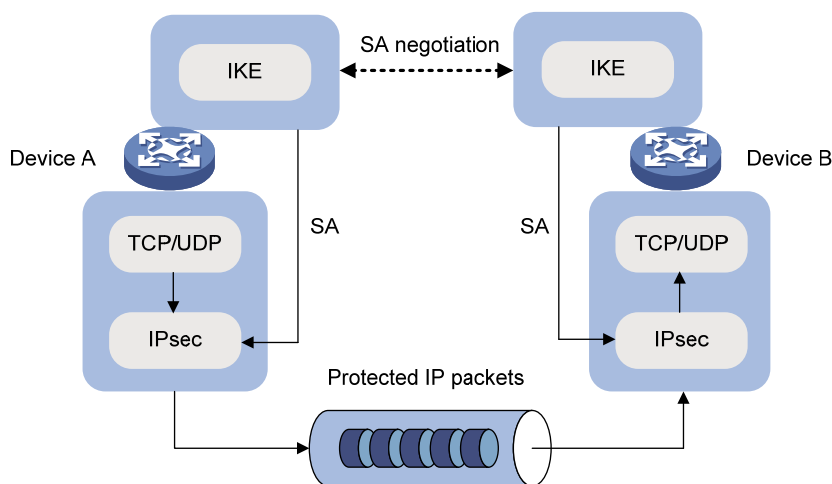
Built on a framework defined by ISAKMP, Internet Key Exchange (IKE) provides automatic key negotiation and SA establishment services for IPsec.

IKE provides the following benefits for IPsec:

- Automatically negotiates IPsec parameters.
- Performs DH exchanges to calculate shared keys, making sure each SA has a key that is independent of other keys.
- Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure IPsec can provide the anti-replay service by using the sequence number.

As shown in [Figure 107](#), IKE negotiates SAs for IPsec and transfers the SAs to IPsec, and IPsec uses the SAs to protect IP packets.

Figure 107 Relationship between IKE and IPsec

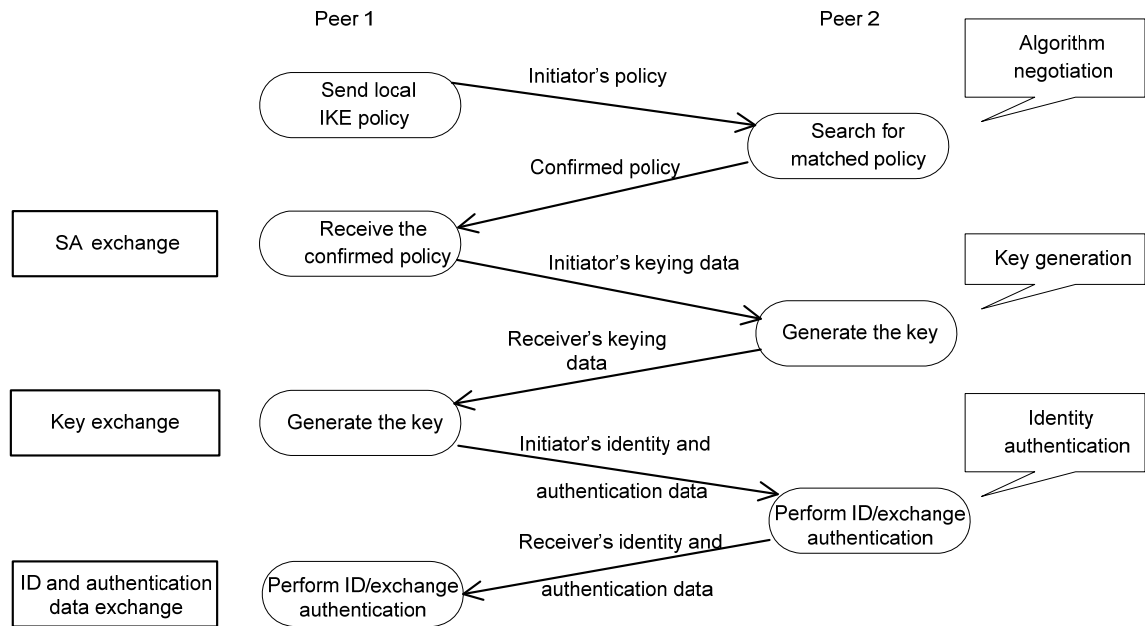


IKE negotiation process

IKE negotiates keys and SAs for IPsec in two phases:

1. **Phase 1**—The two peers establish an IKE SA, a secure, authenticated channel for communication. In this phase, two modes are available: main mode and aggressive mode.
2. **Phase 2**—Using the IKE SA established in phase 1, the two peers negotiate to establish IPsec SAs.

Figure 108 IKE exchange process in main mode



As shown in [Figure 108](#), the main mode of IKE negotiation in phase 1 involves three pairs of messages:

- **SA exchange**—Used for negotiating the IKE security policy.
- **Key exchange**—Used for exchanging the DH public value and other values, such as the random number. The two peers use the exchanged data to generate key data and use the encryption key and authentication key to ensure the security of IP packets.
- **ID and authentication data exchange**—Used for identity authentication.

The main difference between the main mode and the aggressive mode is that the aggressive mode does not provide identity information protection and exchanges only three messages, rather than three pairs. The main mode provides identity information protection but is slower.

IKE security mechanism

IKE has a series of self-protection mechanisms and supports secure identity authentication, key distribution, and IPsec SA establishment on insecure networks.

Identity authentication

The IKE identity authentication mechanism is used to authenticate the identity of the communicating peers. The device supports the following identity authentication methods:

- **Pre-shared key authentication**—Two communicating peers use the pre-configured shared key for identity authentication.
- **RSA signature authentication and DSA signature authentication**—Two communicating peers use the digital certificates issued by the CA for identity authentication.

The pre-shared key authentication method does not require certificates and is easy to configure. It is usually deployed in small networks.

The signature authentication methods provide higher security and are usually deployed in networks with the headquarters and some branches. When deployed in a network with many branches, a signature authentication method can simplify the configuration because only one PKI domain is required. If you use the pre-shared key authentication method, you must configure a pre-shared key for each branch on the Headquarters node.

DH algorithm

The DH algorithm is a public key algorithm. With this algorithm, two peers can exchange keying material and then use the material to calculate the shared keys. Due to the decryption complexity, a third party cannot decrypt the keys even after intercepting all keying materials.

PFS

The Perfect Forward Secrecy (PFS) feature is a security feature based on the DH algorithm. After PFS is enabled, an additional DH exchange is performed in IKE phase 2 to make sure IPsec keys have no derivative relations with IKE keys and a broken key brings no threats to other keys.

Protocols and standards

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2412, *The OAKLEY Key Determination Protocol*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see ["Configuring FIPS"](#)) and non-FIPS mode.

IKE configuration prerequisites

Determine the following parameters prior to IKE configuration:

- The algorithms to be used during IKE negotiation, including the identity authentication method, encryption algorithm, authentication algorithm, and DH group.
 - Different algorithms provide different levels of protection. A stronger algorithm provides more resistance to decryption but uses more resources.
 - A DH group that uses more bits provides higher security but needs more time for processing.
- The pre-shared key or PKI domain for IKE negotiation. For more information about PKI, see ["Configuring PKI."](#)
- The IKE-based IPsec policies for the communicating peers. If no IKE profile is specified for an IPsec policy, the device selects an IKE profile for the IPsec policy. If no IKE profile is configured, the globally configured IKE settings are used. For more information about IPsec, see ["Configuring IPsec."](#)

IKE configuration task list

Tasks at a glance	Remarks
(Optional.) Configuring an IKE profile	N/A
(Optional.) Configuring an IKE proposal	Required when you specify IKE proposals for the IKE profile.
(Optional.) Configuring an IKE keychain	Required when pre-shared authentication is used in IKE negotiation phase 1.
(Optional.) Configuring the global identity information	N/A

Tasks at a glance	Remarks
(Optional.) Configuring the IKE keepalive function	N/A
(Optional.) Configuring the IKE NAT keepalive function	N/A
(Optional.) Configuring IKE DPD	N/A
(Optional.) Enabling invalid SPI recovery	N/A
(Optional.) Setting the maximum number of IKE SAs	N/A
(Optional.) Configuring SNMP notifications for IKE	N/A

Configuring an IKE profile

An IKE profile is intended to provide a set of parameters for IKE negotiation. To configure an IKE profile, you can do the following:

1. Configure peer IDs. When an end needs to select an IKE profile, it compares the received peer ID with the peer IDs of its local IKE profiles. If a match is found, it uses the IKE profile with the matching peer ID for IKE negotiation.
2. Configure the IKE keychain or PKI domain for the IKE proposals to use:
 - o To use digital signature authentication, configure a PKI domain.
 - o To use pre-shared key authentication, configure an IKE keychain.
3. Specify the negotiation mode (main or aggressive) that the device uses as the initiator. When the device acts as the responder, it uses the IKE negotiation mode of the initiator.
4. Specifies the IKE proposals that the device can use as the initiator. An IKE proposal specified earlier has a higher priority. When the device acts as the responder, it uses the IKE proposals configured in system view to match the IKE proposals received from the initiator. If a match is not found, the negotiation fails.
5. Configure the local ID, the ID that the device uses to identify itself to the peer during IKE negotiation:
 - o For digital signature authentication, the device can use an ID of any type. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN (the device name configured by using the **sysname** command) instead.
 - o For pre-shared key authentication, the device can use an ID of any type other than the DN.
6. Configure IKE DPD to detect dead IKE peers. You can also configure this feature in system view. The IKE DPD settings configured in the IKE profile view takes precedence over those configured in system view.
7. Specify a local interface or IP address for the IKE profile so the profile can be applied only to the specified interface or IP address. For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command). If no local address is configured, specify the IP address of the interface to which the IPsec policy is applied.
8. Specify an inside VPN instance. This setting determines where the device should forward received IPsec protected data. If you specify an inside VPN instance, the device looks for a route in the specified VPN instance to forward the data. Otherwise, the device looks for a route in the VPN instance where the receiving interface resides and forwards the data to the VPN instance.
9. Specify a priority number for the IKE profile. To determine the priority of an IKE profile:
 - a. First, the device examines the existence of the **match local address** command. An IKE profile with the **match local address** command configured has a higher priority.
 - b. If a tie exists, the device compares the priority numbers. An IKE profile with a smaller priority number has a higher priority.
 - c. If a tie still exists, the device prefers an IKE profile configured earlier.

To configure an IKE profile:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKE profile and enter its view.	ike profile <i>profile-name</i>	By default, no IKE profile is configured.
3. Configure a peer ID.	match remote { certificate <i>policy-name</i> identity { address { { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] range <i>low-ipv4-address high-ipv4-address</i> } } ipv6 { <i>ipv6-address</i> [<i>prefix-length</i>] range <i>low-ipv6-address high-ipv6-address</i> } } } [vpn-instance <i>vpn-name</i>] fqdn <i>fqdn-name</i> user-fqdn <i>user-fqdn-name</i> } }	By default, an IKE profile has no peer ID. Each of the two peers must have at least one peer ID configured.
4. Specify the keychain for pre-shared key authentication or the PKI domain used to request a certificate for digital signature authentication.	- To specify the keychain for pre-shared key authentication: keychain <i>keychain-name</i> - To specify the PKI domain used to request a certificate for digital signature authentication: certificate domain <i>domain-name</i>	Configure at least one command as required. By default, no IKE keychain or PKI domain is specified for an IKE profile.
5. Specify the IKE negotiation mode for phase 1.	- In non-FIPS mode: exchange-mode { aggressive main } - In FIPS mode: exchange-mode main	By default, the main mode is used during IKE negotiation phase 1.
6. Specify IKE proposals for the IKE profile.	proposal <i>proposal-number</i> <1-6>	By default, no IKE proposals are specified for an IKE profile and the IKE proposals configured in system view are used for IKE negotiation.
7. Configure the local ID.	local-identity { address { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } dn fqdn [<i>fqdn-name</i>] user-fqdn [<i>user-fqdn-name</i>] }	By default, no local ID is configured for an IKE profile, and an IKE profile uses the local ID configured in system view. If the local ID is not configured in system view, the IKE profile uses the IP address of the interface to which the IPsec policy or IPsec policy template is applied as the local ID.
8. (Optional.) Configure IKE DPD.	dpd interval <i>interval-seconds</i> [retry <i>seconds</i>] { on-demand periodic }	By default, IKE DPD is not configured for an IKE profile and an IKE profile uses the DPD settings configured in system view. If IKE DPD is not configured in system view either, the device does not perform dead IKE peer detection.

Step	Command	Remarks
9. (Optional.) Specify the local interface or IP address to which the IKE profile can be applied.	match local address { <i>interface-type interface-number</i> { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-name</i>] }	By default, an IKE profile can be applied to any local interface or IP address.
10. (Optional.) Specify an inside VPN instance.	inside-vpn <i>vpn-instance</i> <i>vpn-name</i>	By default, no inside VPN instance is specified for an IKE profile, and the device forwards protected data to the VPN instance where the interface receiving the data resides.
11. (Optional.) Specify a priority for the IKE profile.	priority <i>number</i>	By default, the priority of an IKE profile is 100.

Configuring an IKE proposal

An IKE proposal defines a set of attributes describing how IKE negotiation in phase 1 should take place. You can create multiple IKE proposals with different priorities. The priority of an IKE proposal is represented by its sequence number. The lower the sequence number, the higher the priority.

Two peers must have at least one matching IKE proposal for successful IKE negotiation. During IKE negotiation:

- The initiator sends its IKE proposals to the peer.
 - If the initiator is using an IPsec policy with an IKE profile, the initiator sends all IKE proposals in the IKE profile to the peer. An IKE proposal specified earlier for the IKE profile has a higher priority.
 - If the initiator is using an IPsec policy with no IKE profile, the initiator sends all its IKE proposals to the peer. An IKE proposal with a smaller number has a higher priority.
- The peer searches its own IKE proposals for a match. The search starts from the IKE proposal with the highest priority and proceeds in descending order of priority until a match is found. The matching IKE proposals are used to establish the IKE SA. If all user-defined IKE proposals are found mismatching, the two peers use their default IKE proposals to establish the IKE SA.

Two matching IKE proposals have the same encryption algorithm, authentication method, authentication algorithm, and DH group. The SA lifetime takes the smaller one of the two proposals' SA lifetime settings.

To configure an IKE proposal:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKE proposal and enter its view.	ike proposal <i>proposal-number</i>	By default, there is an IKE proposal that is used as the default IKE proposal.

Step	Command	Remarks
3. Specify an encryption algorithm for the IKE proposal.	- In non-FIPS mode: encryption-algorithm { 3des-cbc aes-cbc-128 aes-cbc-192 aes-cbc-256 des-cbc sm1-cbc-128 sm1-cbc-192 sm1-cbc-256 sm4-cbc } - In FIPS mode: encryption-algorithm { aes-cbc-128 aes-cbc-192 aes-cbc-256 }	By default: - In non-FIPS mode, an IKE proposal uses the 56-bit DES encryption algorithm in CBC mode. - In FIPS mode, an IKE proposal uses the 128-bit AES encryption algorithm in CBC mode.
4. Specify an authentication method for the IKE proposal.	authentication-method { dsa-signature pre-share rsa-signature }	By default, an IKE proposal uses the pre-shared key authentication method.
5. Specify an authentication algorithm for the IKE proposal.	- In non-FIPS mode: authentication-algorithm { md5 sha sm3 } - In FIPS mode: authentication-algorithm sha	By default, an IKE proposal uses the HMAC-SHA1 authentication algorithm.
6. Specify a DH group for key negotiation in phase 1.	- In non-FIPS mode: dh { group1 group14 group2 group24 group5 } - In FIPS mode: dh group14	By default: - In non-FIPS mode, DH group1 (the 768-bit DH group) is used. - In FIPS mode, DH group14 (the 2048-bit DH group) is used.
7. Set the IKE SA lifetime for the IKE proposal.	sa duration <i>seconds</i>	By default, the IKE SA lifetime is 86400 seconds.

Configuring an IKE keychain

Perform this task when you configure the IKE to use the pre-shared key for authentication.

Follow these guidelines when you configure an IKE keychain:

- Two peers must be configured with the same pre-shared key to pass pre-shared key authentication.
- You can specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for the IKE keychain to be applied. If no local address is configured, specify the IP address of the interface to which the IPsec policy is applied.
- You can specify a priority number for the IKE keychain. To determine the priority of an IKE keychain:
 - The device examines the existence of the **match local address** command. An IKE keychain with the **match local address** command configured has a higher priority.
 - If a tie exists, the device compares the priority numbers. An IKE keychain with a smaller priority number has a higher priority.
 - If a tie still exists, the device prefers an IKE keychain configured earlier.

To configure the IKE keychain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Create an IKE keychain and enter its view.	ike keychain <i>keychain-name</i> [vpn-instance <i>vpn-name</i>]	By default, no IKE keychain exists.
3. Configure a pre-shared key.	- In non-FIPS mode: pre-shared-key { address { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] ipv6 <i>ipv6-address</i> [<i>prefix-length</i>] } hostname <i>host-name</i> } key { cipher <i>cipher-key</i> simple <i>simple-key</i> } - In FIPS mode: pre-shared-key { address { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] ipv6 <i>ipv6-address</i> [<i>prefix-length</i>] } hostname <i>host-name</i> } key [cipher <i>cipher-key</i>]	By default, no pre-shared key is configured. For security purposes, all pre-shared keys, including those configured in plain text, are saved in cipher text to the configuration file.
4. (Optional.) Specify a local interface or IP address to which the IKE keychain can be applied.	match local address { <i>interface-type</i> <i>interface-number</i> { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } } [vpn-instance <i>vpn-name</i>] }	By default, an IKE keychain can be applied to any local interface or IP address.
5. (Optional.) Specify a priority for the IKE keychain.	priority <i>number</i>	The default priority is 100.

Configuring the global identity information

Follow these guidelines when you configure the global identity information for the local IKE:

- The global identity can be used by the device for all IKE SA negotiations, and the local identity (set by the **local-identity** command) can be used only by the device that uses the IKE profile.
- When signature authentication is used, you can set any type of the identity information.
- When pre-shared key authentication is used, you cannot set the DN as the identity.

To configure the global identity information:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the global identity to be used by the local end.	ike identity { address { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } dn fqdn [<i>fqdn-name</i>] user-fqdn [<i>user-fqdn-name</i>] }	By default, the IP address of the interface to which the IPsec policy or IPsec policy template is applied is used as the IKE identity.

Step	Command	Remarks
3. (Optional.) Configure the local device to always obtain the identity information from the local certificate for signature authentication.	ike signature-identity from-certificate	By default, the local end uses the identity information specified by local-identity or ike identity for signature authentication. Configure this command on the local device when the following conditions exist: • If the aggressive IKE SA negotiation mode and signature authentication are used. • When the device interconnects with a peer device that runs a Comware 5-based release supporting only DN for signature authentication.

Configuring the IKE keepalive function

IKE sends keepalive packets to query the liveness of the peer. If the peer is configured with the keepalive timeout time, you must configure the keepalive interval on the local device. If the peer receives no keepalive packets during the timeout time, the IKE SA is deleted along with the IPsec SAs it negotiated.

Follow these guidelines when you configure the IKE keepalive function:

- Configure IKE DPD instead of the IKE keepalive function unless IKE DPD is not supported on the peer. The IKE keepalive function sends keepalives at regular intervals, which consumes network bandwidth and resources.
- The keepalive timeout time configured on the local device must be longer than the keepalive interval configured at the peer. Since it seldom occurs that more than three consecutive packets are lost on a network, you can set the keepalive timeout three times as long as the keepalive interval.

To configure the IKE keepalive function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the IKE SA keepalive interval.	ike keepalive interval <i>seconds</i>	By default, no keepalives are sent to the peer.
3. Set the IKE SA keepalive timeout time.	ike keepalive timeout <i>seconds</i>	By default, IKE SA keepalive never times out.

Configuring the IKE NAT keepalive function

If IPsec traffic passes through a NAT device, you must configure the NAT traversal function. If no packet travels across an IPsec tunnel in a period of time, the NAT sessions are aged and deleted, disabling the tunnel from transmitting data to the intended end. To prevent NAT sessions from being aged, configure the NAT keepalive function on the IKE gateway behind the NAT device to send NAT keepalive packets to its peer periodically to keep the NAT session alive.

To configure the IKE NAT keepalive function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the IKE NAT keepalive interval.	ike nat-keepalive <i>seconds</i>	The default interval is 20 seconds.

Configuring IKE DPD

DPD detects dead peers. It can operate in periodic mode or on-demand mode.

- **Periodic DPD**—Sends a DPD message at regular intervals. It features an earlier detection of dead peers, but consumes more bandwidth and CPU.
- **On-demand DPD**—Sends a DPD message based on traffic. When the device has traffic to send and is not aware of the liveness of the peer, it sends a DPD message to query the status of the peer. If the device has no traffic to send, it never sends DPD messages. As a best practice, use this mode.

The IKE DPD works as follows:

1. The local device sends a DPD message to the peer, and waits for a response from the peer.
2. If the peer does not respond within the retry interval specified by the **retry seconds** parameter, the local device resends the message.
3. If still no response is received within the retry interval, the local end sends the DPD message again. The system allows a maximum of two retries.
4. If the local device receives no response after two retries, the device considers the peer to be dead, and deletes the IKE SA along with the IPsec SAs it negotiated.
5. If the local device receives a response from the peer during the detection process, the peer is considered alive. The local device performs a DPD detection again when the triggering interval is reached or it has traffic to send, depending on the DPD mode.

Follow these guidelines when you configure the IKE DPD function:

- When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.
- It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection is not triggered during a DPD retry.

To configure IKE DPD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable sending IKE DPD messages.	ike dpd interval <i>interval-seconds</i> [retry seconds] { on-demand periodic }	By default, IKE DPD is disabled.

Enabling invalid SPI recovery

An IPsec "black hole" occurs when one IPsec peer fails (for example, a peer can fail if a reboot occurs). One peer fails and loses its SAs with the other peer. When an IPsec peer receives a data packet for which it cannot find an SA, an invalid SPI is encountered. The peer drops the data packet and tries to send an SPI invalid notification to the data originator. This notification is sent by using the IKE SA. Because no IKE SA is available, the notification is not sent. The originating peer continues

sending the data by using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic.

The invalid SPI recovery feature enables the receiving peer to set up an IKE SA with the originator so that an SPI invalid notification can be sent. Upon receiving the notification, the originating peer deletes the IPsec SA that has the invalid SPI. If the originator has data to send, new SAs will be set up.

Use caution when you enable the invalid SPI recovery feature because using this feature can result in a DoS attack. Attackers can make a great number of invalid SPI notifications to the same peer.

To enable invalid SPI recovery:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable invalid SPI recovery.	ike invalid-spi-recovery enable	By default, the invalid SPI recovery is disabled.

Setting the maximum number of IKE SAs

You can set the maximum number of half-open IKE SAs and the maximum number of established IKE SAs.

- The supported maximum number of half-open IKE SAs depends on the device's processing capability. Adjust the maximum number of half-open IKE SAs to make full use of the device's processing capability without affecting the IKE SA negotiation efficiency.
- The supported maximum number of established IKE SAs depends on the device's memory space. Adjust the maximum number of established IKE SAs to make full use of the device's memory space without affecting other applications in the system.

To set the limit on the number of IKE SAs:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the maximum number of half-open IKE SAs and the maximum number of established IKE SAs.	ike limit { max-negotiating-sa negotiation-limit max-sa sa-limit }	By default, there is no limit to the maximum number of IKE SAs.

Configuring SNMP notifications for IKE

After you enable SNMP notifications for IKE, the IKE module notifies the NMS of important module events. The notifications are sent to the device's SNMP module. You can configure the notification transmission parameters for the SNMP module to specify how the SNMP module displays notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To generate and output SNMP notifications for a specific IKE failure or event type, perform the following tasks:

1. Enable SNMP notifications for IKE globally.
2. Enable SNMP notifications for the failure or event type.

To configure SNMP notifications for IKE:

Step	Command	Remarks
1. Enter system view	system-view	N/A
2. Enable SNMP notifications for IKE globally.	snmp-agent trap enable ike global	By default, SNMP notifications for IKE are enabled.
3. Enable SNMP notifications for the specified failure or event types.	snmp-agent trap enable ike [attr-not-support auth-failure cert-type-unsupported cert-unavailable decrypt-failure encrypt-failure invalid-cert-auth invalid-cookie invalid-id invalid-proposal invalid-protocol invalid-sign no-sa-failure proposal-add proposal-delete tunnel-start tunnel-stop unsupported-exch-type] *	By default, SNMP notifications for all failure and event types are enabled.

Displaying and maintaining IKE

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display configuration information about all IKE proposals.	display ike proposal
Display information about the current IKE SAs.	display ike sa [verbose [connection-id <i>connection-id</i> remote-address [ipv6] <i>remote-address</i> [vpn-instance <i>vpn-name</i>]]]
Delete IKE SAs.	reset ike sa [connection-id <i>connection-id</i>]
Clear IKE MIB statistics.	reset ike statistics

IKE configuration examples

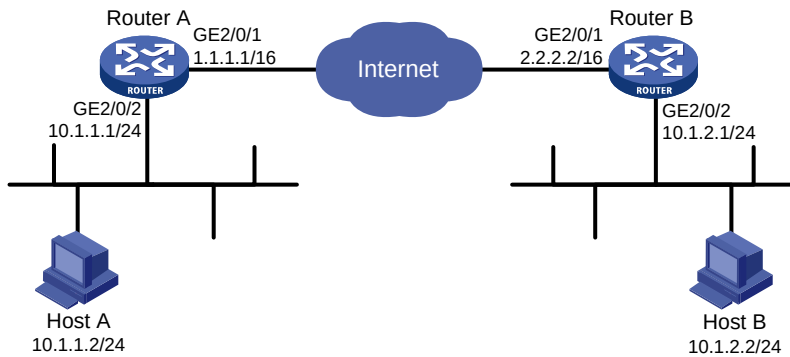
Main mode IKE with pre-shared key authentication configuration example

Network requirements

As shown in [Figure 109](#), configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

Configure Device A and Device B to use the default IKE proposal for the IKE negotiation to set up the IPsec SAs. Configure the two devices to use the pre-shared key authentication method for the IKE negotiation phase 1.

Figure 109 Network diagram



Configuration procedure

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3101
```

```
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[DeviceA] ipsec transform-set tran1
```

Set the packet encapsulation mode to **tunnel**.

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Use the ESP protocol for the IPsec transform set.

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

Specify the encryption and authentication algorithms.

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

```
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[DeviceA-ipsec-transform-set-tran1] quit
```

Create an IKE keychain named **keychain1**.

```
[DeviceA] ike keychain keychain1
```

Specify plaintext **123456TESTplat&!** as the pre-shared key to be used with the remote peer at 2.2.2.2.

```
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.255.0 key simple 123456TESTplat&!
```

```
[DeviceA-ike-keychain-keychain1] quit
```

Create an IKE profile named **profile1**.

```
[DeviceA] ike profile profile1
```

Specify IKE keychain **keychain1**.

```
[DeviceA-ike-profile-profile1] keychain keychain1
```

Configure the local ID with the identity type as IP address and the value as **1.1.1.1**.

```
[DeviceA-ike-profile-profile1] local-identity address 1.1.1.1
```

Configure a peer ID with the identity type as IP address and the value as **2.2.2.2/24**.

```
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
```

```
[DeviceA-ike-profile-profile1] quit
```

```

# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
[DeviceA] ipsec policy map1 10 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# Specify IPsec transform set tran1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# Specify IKE profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
# Apply IPsec policy map1 to interface GigabitEthernet 2/0/1.
[DeviceA-GigabitEthernet2/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet2/0/1] quit
# Configure a static route to subnet 10.1.2.0/24.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2

```

2. Configure Device B:

```

# Assign IP addresses to each interface. (Details not shown.)
# Configure ACL 3101 to identify traffic from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<DeviceB> system-view
[DeviceB] acl advanced 3101
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3101] quit
# Create an IPsec transform set named tran1.
[DeviceB] ipsec transform-set tran1
# Set the packet encapsulation mode to tunnel.
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-tran1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
# Create and IKE keychain named keychain1.
[DeviceB]ike keychain keychain1
# Specify plaintext 123456TESTplat&! as the pre-shared key to be used with the remote peer
at 1.1.1.1.
[DeviceB-ike-keychain-keychain1] pre-shared-key address 1.1.1.1 255.255.255.0 key
simple 123456TESTplat&!
[DeviceB-ike-keychain-keychain1] quit
# Create an IKE profile named profile1.
[DeviceB] ike profile profile1
# Specify IKE keychain keychain1
[DeviceB-ike-profile-profile1] keychain keychain1
# Configure the local ID with the identity type as IP address and the value as 2.2.2.2.
[DeviceB-ike-profile-profile1] local-identity address 2.2.2.2

```

```

# Configure a peer ID with the identity type as IP address and the value as 1.1.1.1/24.
[DeviceB-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.255.0
[DeviceB-ike-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 10.
[DeviceB] ipsec policy use1 10 isakmp
# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[DeviceB-ipsec-policy-isakmp-use1-10] remote-address 1.1.1.1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceB-ipsec-policy-isakmp-use1-10] security acl 3101
# Specify IPsec transform set tran1 for the IPsec policy.
[DeviceB-ipsec-policy-isakmp-use1-10] transform-set tran1
# Specify IKE profile profile1 for the IPsec policy.
[DeviceB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[DeviceB-ipsec-policy-isakmp-use1-10] quit
# Apply IPsec policy use1 to interface GigabitEthernet 2/0/1.
[DeviceB-GigabitEthernet2/0/1] ipsec apply policy use1
[DeviceB-GigabitEthernet2/0/1] quit
# Configure a static route to the subnet where Host A resides.
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, traffic between the two subnets is IPsec protected.

Display the IKE proposal configuration on Device A and Device B. Because no IKE proposal is configured, the command displays the default IKE proposal.

```

[DeviceA] display ike proposal

```

	Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
default	PRE-SHARED-KEY	SHA1	AES-CBC-128	Group 1	86400	

```

[DeviceB] display ike proposal

```

	Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
default	PRE-SHARED-KEY	SHA1	AES-CBC-128	Group 1	86400	

Display the IKE SA on Device A.

```

[DeviceA] display ike sa

```

Connection-ID	Remote	Flag	DOI
1	2.2.2.2	RD	IPSEC

Flags:

RD--READY RL--REPLACED FD-FADING

Display the IPsec SAs generated on Device A.

```

[DeviceA] display ipsec sa
-----
Interface: GigabitEthernet2/0/1
-----

```



```

-----
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1456
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2

Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 3264152513 (0xc28f03c1)
Connection ID: 1
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 738451674 (0x2c03e0da)
Connection ID: 2
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
UDP encapsulation used for NAT traversal: N
Status: Active

# Display the IKE SA and IPsec SAs on Device B.
[DeviceB] display ike sa
[DeviceB] display ipsec sa

```

Aggressive mode with RSA signature authentication configuration example

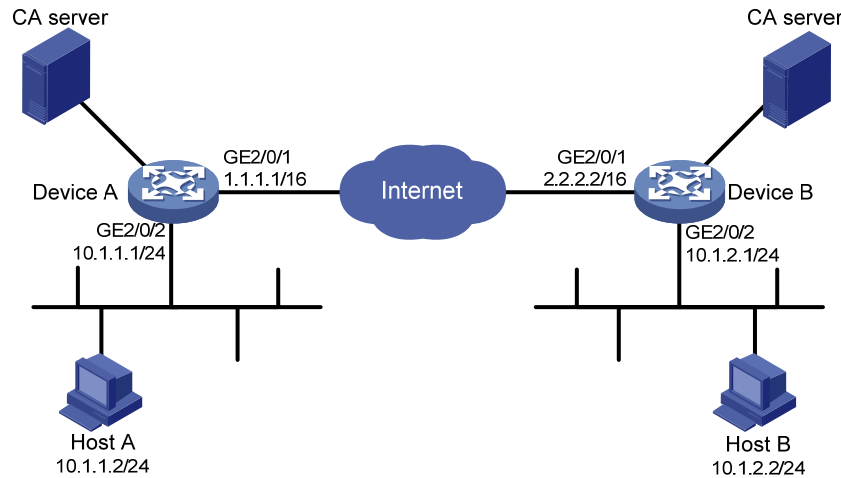
This configuration example is not available when the device is operating in FIPS mode.

Network requirements

As shown in [Figure 110](#), configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

Configure Device A and Device B to use aggressive mode for IKE negotiation phase 1 and use RSA signature authentication. Device A acts as the initiator because the subnet where Device A resides is dynamically allocated.

Figure 110 Network diagram



Configuration procedure

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3101
```

```
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[DeviceA] ipsec transform-set tran1
```

Set the packet encapsulation mode to **tunnel**.

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Use the ESP protocol for the IPsec transform set.

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

Specify the encryption and authentication algorithms.

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
```

```
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[DeviceA-ipsec-transform-set-tran1] quit
```

Create a PKI entity named **entity1**.

```
[DeviceA] pki entity entity1
```

Set the common name as **routera** for the PKI entity.

```
[DeviceA-pki-entity-entity1] common-name routera
```

```
[DeviceA-pki-entity-entity1] quit
```

Create a PKI domain named **domain1**.

```
[DeviceA] pki domain domain1
```

```

# Set the certificate request mode to auto and set the password to 123 for certificate revocation.
[DeviceA-pki-domain-domain1] certificate request mode auto password simple 123
# Set an MD5 fingerprint for verifying the validity of the CA root certificate.
[DeviceA-pki-domain-domain1] root-certificate fingerprint md5
50c7a2d282ea710a449eede6c56b102e
# Specify the trusted CA 8088.
[DeviceA-pki-domain-domain1] ca identifier 8088
# Specify the URL of the registration server for certificate request through the SCEP protocol.
This example uses the URL of
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7.
[DeviceA-pki-domain-domain1] certificate request url
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7
# Specify the CA to accept certificate requests.
[DeviceA-pki-domain-domain1] certificate request from ca
# Specify the PKI entity for certificate request as entity1.
[DeviceA-pki-domain-domain1] certificate request entity entity1
# Specify the RSA key pair rsa1 with the general purpose for certificate request.
[DeviceA-pki-domain-domain1] public-key rsa general name rsa1
[DeviceA-pki-domain-domain1] quit
# Create an IKE profile named profile1.
[DeviceA] ike profile profile1
# Specify PKI domain domain1 for the IKE profile.
[DeviceA-ike-profile-profile1] certificate domain domain1
# Specify that IKE negotiation operates in aggressive mode.
[DeviceA-ike-profile-profile1] exchange-mode aggressive
# Set the local identity to the FQDN name www.routera.com.
[DeviceA-ike-profile-profile1] local-identity fqdn www.routera.com
# Configure a peer ID with the identity type of FQDN name and the value of www.routerb.com.
[DeviceA-ike-profile-profile1] match remote identity fqdn www.routerb.com
[DeviceA-ike-profile-profile1] quit
# Create an IKE proposal named 10.
[DeviceA] ike proposal 10
# Specify the authentication algorithm as HMAC-MD5.
[DeviceA-ike-proposal-10] authentication-algorithm md5
# Specify the RSA authentication method.
[DeviceA-ike-proposal-10] authentication-method rsa-signature
[DeviceA-ike-proposal-10] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
[DeviceA] ipsec policy map1 10 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# Specify IPsec transform set tran1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# Specify IKE profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1

```

```

[DeviceA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 2/0/1.
[DeviceA-GigabitEthernet2/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet2/0/1] quit
# Configure a static route to the subnet where Host B resides.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
2. Configure Device B:
# Assign an IP address to each interface. (Details not shown.)
# Create an IPsec transform set named tran1.
<DeviceB> system-view
[DeviceB] ipsec transform-set tran1
# Set the packet encapsulation mode to tunnel.
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-tran1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
# Create a PKI entity named entity2.
[DeviceB] pki entity entity2
# Set the common name as routerb for the PKI entity.
[DeviceB-pki-entity-entity2] common-name routerb
[DeviceA-pki-entity-entity1] quit
# Create a PKI domain named domain2.
[DeviceB] pki domain domain2
# Set the certificate request mode to auto and set the password to 123 for certificate revocation.
[DeviceB-pki-domain-domain2] certificate request mode auto password simple 123
# Set an MD5 fingerprint for verifying the validity of the CA root certificate.
[DeviceB-pki-domain-domain2] root-certificate fingerprint md5
50c7a2d282ea710a449eede6c56b102e
# Specify the trusted CA 8088.
[DeviceB-pki-domain-domain2] ca identifier 8088
# Specify the URL of the registration server for certificate request through the SCEP protocol.
This example uses the URL of
http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7.
[DeviceB-pki-domain-domain2] certificate request url
http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7
# Specify the CA to accept certificate requests.
[DeviceB-pki-domain-domain2] certificate request from ca
# Specify the PKI entity for certificate request as entity2.
[DeviceB-pki-domain-domain2] certificate request entity entity2
# Specify the RSA key pair rsa1 with the general purpose for certificate request.
[DeviceB-pki-domain-domain2] public-key rsa general name rsa1
[DeviceB-pki-domain-domain2] quit
# Create an IKE profile named profile2.
[DeviceB] ike profile profile2

```

```

# Set the local identity to the FQDN name www.routerb.com.
[DeviceB-ike-profile-profile2] local-identity identity fqdn www.routerb.com
# Configure a peer ID with the identity type of FQDN name and the value of www.routera.com.
[DeviceB-ike-profile-profile2] match remote identity fqdn www.routera.com
[DeviceB-ike-profile-profile2] quit
# Create an IKE proposal named 10.
[DeviceB] ike proposal 10
# Specify the authentication algorithm as HMAC-MD5.
[DeviceB-ike-proposal-10] authentication-algorithm md5
# Specify the RSA authentication method.
[DeviceB-ike-proposal-10] authentication-method rsa-signature
[DeviceB-ike-proposal-10] quit
# Create an IPsec policy template with the name template1 and the sequence number 1.
[DeviceB] ipsec policy-template template1 1
# Specify IPsec transform set tran1 for the IPsec policy template.
[DeviceB-ipsec-policy-template-template1-1] transform-set tran1
[DeviceB-ipsec-policy-template-template1-1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 1 by
referencing the IPsec policy template template1.
[DeviceB] ipsec policy use1 1 isakmp template template1
# Apply IPsec policy use1 to interface GigabitEthernet 2/0/1.
[DeviceB-GigabitEthernet2/0/1] ipsec apply policy use1
[DeviceB-GigabitEthernet2/0/1] quit
# Configure a static route to the subnet where Host A resides.
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, traffic between the two subnets is IPsec protected.

Display the IKE proposal configuration on Device A and Device B.

```

[DeviceA] display ike proposal 10

```

Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
10	RSA-SIG	MD5	AES-CBC-128	Group 1	86400
default	PRE-SHARED-KEY	SHA1	AES-CBC-128	Group 1	86400

```

[DeviceB] display ike proposal 10

```

Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
10	RSA-SIG	MD5	AES-CBC-128	Group 1	86400
default	PRE-SHARED-KEY	SHA1	AES-CBC-128	Group 1	86400

Display the IKE SA on Device A.

```

[DeviceA] display ike sa

```

Connection-ID	Remote	Flag	DOI
1	2.2.2.2	RD	IPSEC

Flags:

RD--READY RL--REPLACED FD-FADING

Display information about the CA certificate on Device A.

[DeviceA] display pki certificate domain domain1 ca

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

b9:14:fb:25:c9:08:2c:9d:f6:94:20:30:37:4e:00:00

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=rnd, OU=sec, CN=8088

Validity

Not Before: Sep 6 01:53:58 2012 GMT

Not After : Sep 8 01:50:58 2015 GMT

Subject: C=cn, O=rnd, OU=sec, CN=8088

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:de:81:f4:42:c6:9f:c2:37:7b:21:84:57:d6:42:

00:69:1c:4c:34:a4:5e:bb:30:97:45:2b:5e:52:43:

c0:49:1f:e1:d8:0f:5c:48:c2:39:69:d1:84:e4:14:

70:3d:98:41:28:1c:20:a1:9a:3f:91:67:78:77:27:

d9:08:5f:7a:c4:36:45:8b:f9:7b:e7:7d:6a:98:bb:

4e:a1:cb:2c:3d:92:66:bd:fb:80:35:16:c6:35:f0:

ff:0b:b9:3c:f3:09:94:b7:d3:6f:50:8d:83:f1:66:

2f:91:0b:77:a5:98:22:b4:77:ac:84:1d:03:8e:33:

1b:31:03:78:4f:77:a0:db:af

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

9a:6d:8c:46:d3:18:8a:00:ce:12:ee:2b:b0:aa:39:5d:3f:90:

08:49:b9:a9:8f:0d:6e:7b:e1:00:fb:41:f5:d4:0c:e4:56:d8:

7a:a7:61:1d:2b:b6:72:e3:09:0b:13:9d:fa:c8:fc:c4:65:a7:

f9:45:21:05:75:2c:bf:36:7b:48:b4:4a:b9:fe:87:b9:d8:cf:

55:16:87:ec:07:1d:55:5a:89:74:73:68:5e:f9:1d:30:55:d9:

8a:8f:c5:d4:20:7e:41:a9:37:57:ed:8e:83:a7:80:2f:b8:31:

57:3a:f2:1a:28:32:ea:ea:c5:9a:55:61:6a:bc:e5:6b:59:0d:

82:16

Display the local certificate on Device A.

[DeviceA] display pki certificate domain domain1 local

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

a1:f4:d4:fd:cc:54:c3:07:c4:9e:15:2d:5f:64:57:77

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=rnd, OU=sec, CN=8088

Validity

Not Before: Sep 26 02:06:43 2012 GMT
Not After : Sep 26 02:06:43 2013 GMT
Subject: CN=devicea
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:b0:a1:cd:24:6e:1a:1d:51:79:f0:2a:3e:9f:e9:
84:07:16:78:49:1b:7d:0b:22:f0:0a:ed:75:91:a4:
17:fd:c7:ef:d0:66:5c:aa:e3:2a:d9:71:12:e4:c6:
25:77:f0:1d:97:bb:92:a8:bd:66:f8:f8:e8:d5:0d:
d2:c8:01:dd:ea:e6:e0:80:ad:db:9d:c8:d9:5f:03:
2d:22:07:e3:ed:cc:88:1e:3f:0c:5e:b3:d8:0e:2d:
ea:d6:c6:47:23:6a:11:ef:3c:0f:6b:61:f0:ca:a1:
79:a0:b1:02:1a:ae:8c:c9:44:e0:cf:d1:30:de:4c:
f0:e5:62:e7:d0:81:5d:de:d3
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 CRL Distribution Points:

Full Name:
URI:http://xx.rsa.com:447/8088.crl

Signature Algorithm: sha1WithRSAEncryption
73:ac:66:f9:b8:b5:39:e1:6a:17:e4:d0:72:3e:26:9e:12:61:
9e:c9:7a:86:6f:27:b0:b9:a3:5d:02:d9:5a:cb:79:0a:12:2e:
cb:e7:24:57:e6:d9:77:12:6b:7a:cf:ee:d6:17:c5:5f:d2:98:
30:e0:ef:00:39:4a:da:ff:1c:29:bb:2a:5b:60:e9:33:8f:78:
f9:15:dc:a5:a3:09:66:32:ce:36:cd:f0:fe:2f:67:e5:72:e5:
21:62:85:c4:07:92:c8:f1:d3:13:9c:2e:42:c1:5f:0e:8f:ff:
65:fb:de:7c:ed:53:ab:14:7a:cf:69:f2:42:a4:44:7c:6e:90:
7e:cd

Display the IPsec SA information on Device A.

[DeviceA] display ipsec sa

Interface: GigabitEthernet2/0/1

IPsec policy: map1
Sequence number: 10
Mode: ISAKMP

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1456
Tunnel:

```
local address: 1.1.1.1
remote address: 2.2.2.2
Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
SPI: 3264152513 (0xc28f03c1)
Connection ID: 1
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

```
[Outbound ESP SAs]
SPI: 738451674 (0x2c03e0da)
Connection ID: 2
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
UDP encapsulation used for NAT traversal: N
Status: Active
```

Display the information about the CA certificate, local certificate, IKE SA, and IPsec SA on Device B.

```
[DeviceB] display ike sa
[DeviceB] display pki certificate domain domain2 ca
[DeviceB] display pki certificate domain domain2 local
[DeviceB] display ipsec sa
```

Aggressive mode with NAT traversal configuration example

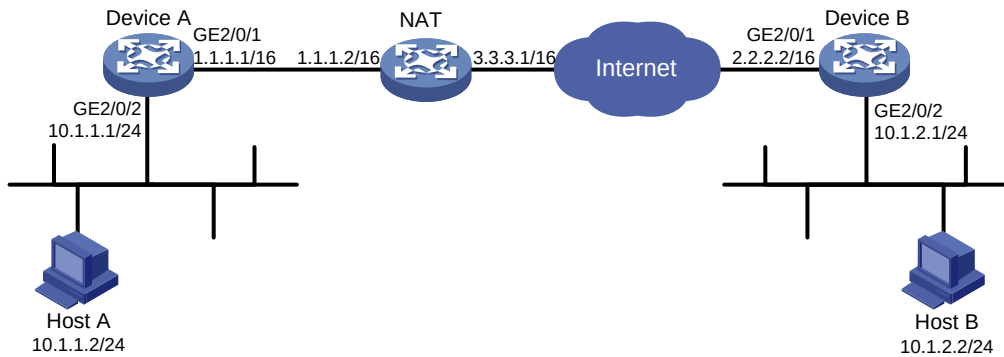
This configuration example is not available when the device is operating in FIPS mode.

Network requirements

Device A is behind the NAT device. Hosts behind Device A use public IP address 3.3.3.1 to access the external network. Configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

Configure Device A and Device B to use the default IKE proposal for the aggressive IKE negotiation to set up the IPsec SAs. Configure the two devices to use the pre-shared key authentication method for the IKE negotiation phase 1.

Figure 111 Network diagram



Configuration procedure

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure ACL 3000 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3000
```

```
[DeviceA-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3000] quit
```

Create an IPsec transform set named **transform1**.

```
[DeviceA] ipsec transform-set transform1
```

Use the ESP protocol for the IPsec transform set.

```
[DeviceA-ipsec-transform-set-transform1] protocol esp
```

Specify the encryption and authentication algorithms.

```
[DeviceA-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
```

```
[DeviceA-ipsec-transform-set-transform1] esp authentication-algorithm md5
```

```
[DeviceA-ipsec-transform-set-transform1] quit
```

Create an IKE keychain named **keychain1**.

```
[DeviceA] ike keychain keychain1
```

Specify plaintext **12345zxcvb!@#%\$ZXCVB** as the pre-shared key to be used with the remote peer at 2.2.2.2.

```
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.255.0 key simple 12345zxcvb!@#%$ZXCVB
```

```
[DeviceA-ike-keychain-keychain1] quit
```

Create an IKE profile named **profile1**.

```
[DeviceA] ike profile profile1
```

Specify IKE keychain **keychain1**.

```
[DeviceA-ike-profile-profile1] keychain keychain1
```

Specify that IKE negotiation operates in aggressive mode.

```
[DeviceA-ike-profile-profile1] exchange-mode aggressive
```

Set the local identity to the FQDN name **www.devicea.com**.

```
[DeviceA-ike-profile-profile1] local-identity fqdn www.devicea.com
```

Configure a peer ID with the identity type as IP address and the value as **2.2.2.2/24**.

```
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
```

```
[DeviceA-ike-profile-profile1] quit
```

```

# Create an IKE-based IPsec policy entry with the name policy1 and the sequence number 1.
[DeviceA] ipsec policy policy1 1 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 2.2.2.2
# Specify IPsec transform set transform1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set transform1
# Specify ACL 3000 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
# Specify IKE profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-policy1-1] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
# Apply IPsec policy policy1 to interface GigabitEthernet 2/0/1.
[DeviceA-GigabitEthernet2/0/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet2/0/1] quit
# Configure a static route to the subnet where Host B resides.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 1.1.1.2

```

2. Configure Device B:

```

# Assign an IP address to each interface. (Details not shown.)
# Create IPsec transform set transform1.
<DeviceB> system-view
[DeviceB] ipsec transform-set transform1
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-transform1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
[DeviceB-ipsec-transform-set-transform1] esp authentication-algorithm md5
[DeviceB-ipsec-transform-set-transform1] quit
# Create IKE keychain keychain1.
[DeviceB]ike keychain keychain1
# Specify plaintext 12345zxcvb!@#$$%ZXCVB as the pre-shared key to be used with the
remote peer at 1.1.1.1. The source address of packets from 1.1.1.1 is translated into 3.3.3.1 by
the NAT device, so specify the IP address of the remote peer as 3.3.3.1.
[DeviceB-ike-keychain-keychain1] pre-shared-key address 3.3.3.1 255.255.255.0 key
simple 12345zxcvb!@#$$%ZXCVB
[DeviceB-ike-keychain-keychain1] quit
# Create an IKE profile named profile1.
[DeviceB] ike profile profile1
# Specify IKE keychain keychain1.
[DeviceB-ike-profile-profile1] keychain keychain1
# Specify that IKE negotiation operates in aggressive mode.
[DeviceB-ike-profile-profile1] exchange-mode aggressive
# Configure a peer ID with the identity type of FQDN name and the value of www.devicea.com.
[DeviceB-ike-profile-profile1] match remote identity fqdn www.devicea.com
[DeviceB-ike-profile-profile1] quit
# Create an IPsec policy template with the name template1 and the sequence number 1.
[DeviceB] ipsec policy-template template1 1
# Specify IPsec transform set transform1 for the IPsec policy template.

```

```

[DeviceB-ipsec-policy-template-template1-1] transform-set transform1
# Specify 2.2.2.2 as the local address of the IPsec tunnel.
[DeviceB-ipsec-policy-template-template1-1] local-address 2.2.2.2
# Specify IKE profile profile1 for the IPsec policy.
[DeviceB-ipsec-policy-template-template1-1] ike-profile profile1
[DeviceB-ipsec-policy-template-template1-1] quit
# Create an IKE-based IPsec policy entry with the name policy1 and the sequence number 1
by referencing the IPsec policy template template1.
[DeviceB] ipsec policy policy1 1 isakmp template template1
# Apply IPsec policy policy1 to interface GigabitEthernet 2/0/1.
[DeviceB-GigabitEthernet2/0/1] ipsec apply policy policy1
[DeviceB-GigabitEthernet2/0/1] quit
# Configure a static route to the subnet where Host A resides.
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 3.3.3.1

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, traffic between the two subnets is IPsec protected.

Display the IKE SA on Device A.

```

[DeviceA] display ike sa

```

Connection-ID	Remote	Flag	DOI
13	2.2.2.2	RD	IPSEC

Flags:

RD--READY RL--REPLACED FD-FADING

```

[DeviceA] display ike sa verbose

```

```

-----
Connection ID: 13
Outside VPN:
Inside VPN:
Profile: profile1
Transmitting entity: Initiator
-----

```

```

Local IP: 1.1.1.1
Local ID type: FQDN
Local ID: www.devicea.com

```

```

Remote IP: 2.2.2.2
Remote ID type: IPV4_ADDR
Remote ID: 2.2.2.2

```

```

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

```

```

Life duration(sec): 86400
Remaining key duration(sec): 84565
Exchange-mode: Aggressive

```

```

Diffie-Hellman group: Group 1
NAT traversal: Detected
# Display the IPsec SAs generated on Device A.
[DeviceA] display ipsec sa
-----

Interface: GigabitEthernet2/0/1
-----

-----
IPsec policy: policy1
Sequence number: 1
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1435
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2
Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 10.2.1.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 830667426 (0x3182faa2)
Connection ID: 1
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/2313
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for nat traversal: Y
Status: Active

[Outbound ESP SAs]
SPI: 3516214669 (0xd1952d8d)
Connection ID: 2
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/2313
Max received sequence-number:
UDP encapsulation used for nat traversal: Y
Status: Active

```

Troubleshooting IKE

IKE negotiation failed because no matching IKE proposals were found

Symptom

1. The IKE SA is in Unknown state.

<Sysname> display ike sa

Connection-ID	Remote	Flag	DOI

1	192.168.222.5	Unknown	IPSEC

Flags:

RD--READY RL--REPLACED FD-FADING

2. When IKE event debugging and packet debugging are enabled, the following messages appear:

IKE event debugging message:

The attributes are unacceptable.

IKE packet debugging message:

Construct notification packet: NO_PROPOSAL_CHOSEN.

Analysis

Certain IKE proposal settings are incorrect.

Solution

1. Examine the IKE proposal configuration to see whether the two ends have matching IKE proposals.
2. Modify the IKE proposal configuration to make sure the two ends have matching IKE proposals.

IKE negotiation failed because no IKE proposals or IKE keychains are specified correctly

Symptom

1. The IKE SA is in Unknown state.

<Sysname> display ike sa

Connection-ID	Remote	Flag	DOI

1	192.168.222.5	Unknown	IPSEC

Flags:

RD--READY RL--REPLACED FD-FADING

2. The following IKE event debugging or packet debugging message appeared:

IKE event debugging message:

Notification PAYLOAD_MALFORMED is received.

IKE packet debugging message:

Construct notification packet: PAYLOAD_MALFORMED.

Analysis

- If the following debugging information appeared, the matched IKE profile is not referencing the matched IKE proposal:
Failed to find proposal 1 in profile profile1.
- If the following debugging information appeared, the matched IKE profile is not referencing the matched IKE keychain:
Failed to find keychain keychain1 in profile profile1.

Solution

- Verify that the matched IKE proposal (IKE proposal 1 in this debugging message example) is specified for the IKE profile (IKE profile 1 in the example).
- Verify that the matched IKE keychain (IKE keychain 1 in this debugging message example) is specified for the IKE profile (IKE profile 1 in the example).

IPsec SA negotiation failed because no matching IPsec transform sets were found

Symptom

1. The **display ike sa** command shows that the IKE SA negotiation succeeded and the IKE SA is in RD state, but the **display ipsec sa** command shows that the expected IPsec SA has not been negotiated yet.
2. The following IKE debugging message appeared:
The attributes are unacceptable.
Or:
Construct notification packet: NO_PROPOSAL_CHOSEN.

Analysis

Certain IPsec policy settings are incorrect.

Solution

1. Examine the IPsec configuration to see whether the two ends have matching IPsec transform sets.
2. Modify the IPsec configuration to make sure the two ends have matching IPsec transform sets.

IPsec SA negotiation failed due to invalid identity information

Symptom

1. The **display ike sa** command shows that the IKE SA negotiation succeeded and the IKE SA is in RD state, but the **display ipsec sa** command shows that the expected IPsec SA has not been negotiated yet.
2. The following IKE debugging message appeared:
Notification INVALID_ID_INFORMATION is received.
Or:
Failed to get IPsec policy when renegotiating IPsec SA. Delete IPsec SA.
Construct notification packet: INVALID_ID_INFORMATION.

Analysis

Certain IPsec policy settings of the responder are incorrect. Verify the settings as follows:

1. Use the **display ike sa verbose** command to verify that matching IKE profiles were found in IKE negotiation phase 1. If no matching IKE profiles were found and the IPsec policy is referencing an IKE profile, the IPsec SA negotiation fails.

Verify that matching IKE profiles were found in IKE negotiation phase 1.

```
<Sysname> display ike sa verbose
```

```
-----
Connection ID: 3
Outside VPN:
Inside VPN:
Profile:
Transmitting entity: Responder
-----

Local IP: 192.168.222.5
Local ID type: IPV4_ADDR
Local ID: 192.168.222.5

Remote IP: 192.168.222.71
Remote ID type: IPV4_ADDR
Remote ID: 192.168.222.71

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400
Remaining key duration(sec): 85847
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected
```

Verify that the IPsec policy is referencing an IKE profile.

```
[Sysname] display ipsec policy
```

```
-----
IPsec Policy: policy1
Interface: GigabitEthernet2/0/1
-----

-----
Sequence number: 1
Mode: isakmp
-----

Description:
Security data flow: 3000
Selector mode: aggregation
Local address: 192.168.222.5
Remote address: 192.168.222.71
Transform set: transform1
IKE profile: profile1
SA duration(time based):
SA duration(traffic based):
```

SA idle time:

2. Verify that the ACL used by the IPsec policy is correctly configured. If the flow range defined by the responder's ACL is smaller than that defined by the initiator's ACL, IPsec proposal matching will fail.

For example, if the initiator's ACL defines a flow from one network segment to another but the responder's ACL defines a flow from one host to another host, IPsec proposal matching will fail.

On the initiator:

```
[Sysname] display acl 3000
```

Advanced ACL 3000, named -none-, 2 rules,

ACL's step is 5

```
rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

On the responder:

```
[Sysname] display acl 3000
```

Advanced ACL 3000, named -none-, 2 rules,

ACL's step is 5

```
rule 0 permit ip source 192.168.222.71 0 destination 192.168.222.5 0
```

3. Verify that the IPsec policy has a remote address and an IPsec transform set configured and that the IPsec transform set has all necessary settings configured.

If, for example, the IPsec policy has no remote address configured, the IPsec SA negotiation will fail:

```
[Sysname] display ipsec policy
```

```
-----  
IPsec Policy: policy1
```

```
Interface: GigabitEthernet2/0/1  
-----
```

```
-----  
Sequence number: 1
```

```
Mode: isakmp  
-----
```

```
Description:
```

```
Security data flow: 3000
```

```
Selector mode: aggregation
```

```
Local address: 192.168.222.5
```

```
Remote address:
```

```
Transform set: transform1
```

```
IKE profile: profile1
```

```
SA duration(time based):
```

```
SA duration(traffic based):
```

```
SA idle time:
```

Solution

1. If the IPsec policy specifies an IKE profile but no matching IKE profiles were found in IKE negotiation, perform one of the following operations on the responder:
 - o Remove the specified IKE profile from the IPsec policy.
 - o Modify the specified IKE profile to match the IKE profile of the initiator.
2. If the flow range defined by the responder's ACL is smaller than that defined by the initiator's ACL, modify the responder's ACL so the ACL defines a flow range equal to or greater than that of the initiator's ACL.

For example:

```
[Sysname] display acl 3000
```

Advanced ACL 3000, named -none-, 2 rules,

ACL's step is 5

```
rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

3. Configure the missing settings (for example, the remote address).

Configuring IKEv2

Overview

Internet Key Exchange version 2 (IKEv2) is an enhanced version of IKEv1. The same as IKEv1, IKEv2 has a set of self-protection mechanisms and can be used on insecure networks for reliable identity authentication, key distribution, and IPsec SA negotiation. IKEv2 provides stronger protection against attacks and higher key exchange ability and needs less message exchanges than IKEv1.

IKEv2 negotiation process

Compared with IKEv1, IKEv2 simplifies the negotiation process and is much more efficient.

IKEv2 defines three types of exchanges: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange.

As shown in [Figure 112](#), IKEv2 uses two exchanges during the initial exchange process: IKE_SA_INIT and IKE_AUTH, each with two messages.

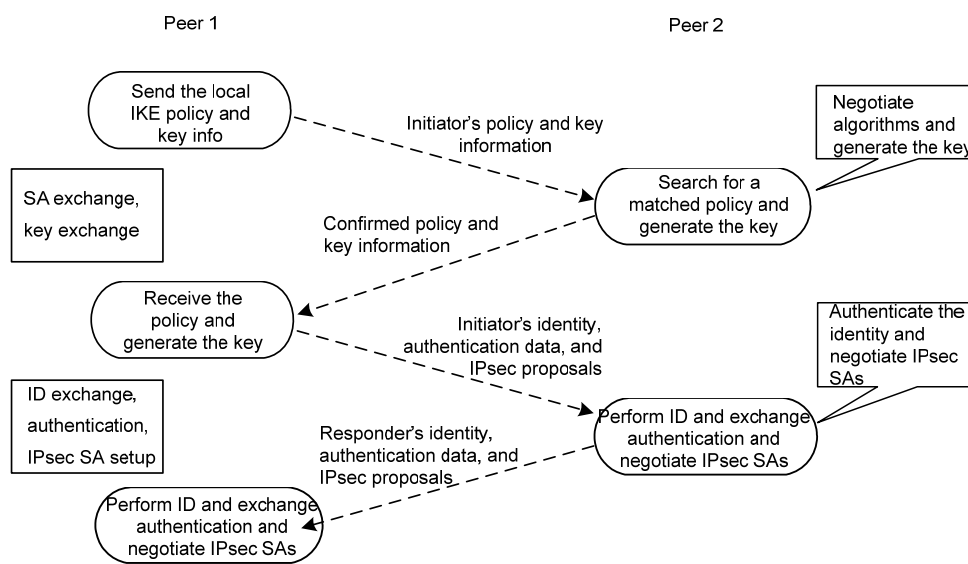
- **IKE_SA_INIT exchange**—Negotiates IKE SA parameters and exchanges keys.
- **IKE_AUTH exchange**—Authenticates the identity of the peer and establishes IPsec SAs.

After the four-message initial exchanges, IKEv2 sets up one IKE SA and one pair of IPsec SAs. For IKEv1 to set up one IKE SA and one pair of IPsec SAs, it must go through two phases that use a minimum of six messages.

To set up one more pair of IPsec SAs within the IKE SA, IKEv2 goes on to perform an additional two-message exchange—the CREATE_CHILD_SA exchange. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and Child SAs.

IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

Figure 112 IKEv2 Initial exchange process



New features in IKEv2

DH guessing

In the IKE_SA_INIT exchange, the initiator guesses the DH group that the responder is most likely to use and sends it in an IKE_SA_INIT request message. If the initiator's guess is correct, the responder responds with an IKE_SA_INIT response message and the IKE_SA_INIT exchange is finished. If the guess is wrong, the responder responds with an INVALID_KEY_PAYLOAD message that contains the DH group that it wants to use. The initiator then uses the DH group selected by the responder to reinitiate the IKE_SA_INIT exchange. The DH guessing mechanism allows for more flexible DH group configuration and enables the initiator to adapt to different responders.

Cookie challenging

Messages for the IKE_SA_INIT exchange are in plain text. An IKEv1 responder cannot confirm the validity of the initiators and must maintain half-open IKE SAs, which makes the responder susceptible to DoS attacks. An attacker can send a large number of IKE_SA_INIT requests with forged source IP addresses to the responder, exhausting the responder's system resources.

IKEv2 introduces the cookie challenging mechanism to prevent such DoS attacks. When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

The cookie challenging mechanism automatically stops working when the number of half-open IKE SAs drops below the threshold.

IKEv2 SA rekeying

For security purposes, both IKE SAs and IPsec SAs have a lifetime and must be rekeyed when the lifetime expires. An IKEv1 SA lifetime is negotiated. An IKEv2 SA lifetime, in contrast, is configured. If two peers are configured with different lifetimes, the peer with the shorter lifetime always initiates the SA rekeying. This mechanism reduces the possibility that two peers will simultaneously initiate a rekeying. Simultaneous rekeying results in redundant SAs and SA status inconsistency on the two peers.

IKEv2 message retransmission

Unlike IKEv1 messages, IKEv2 messages appear in request/response pairs. IKEv2 uses the Message ID field in the message header to identify the request/response pair. If an initiator sends a request but receives no response with the same Message ID value within a specific period of time, the initiator retransmits the request.

It is always the IKEv2 initiator that initiates the retransmission, and the retransmitted message must use the same Message ID value.

Protocols and standards

- RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4718, IKEv2 Clarifications and Implementation Guidelines
- RFC 2412, The OAKLEY Key Determination Protocol
- RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2)

IKEv2 configuration task list

Determine the following parameters prior to IKEv2 configuration:

- The strength of the algorithms for IKEv2 negotiation, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. Different algorithms provide different levels of protection. A stronger algorithm means better resistance to decryption of protected data but requires more resources. Typically, the longer the key, the stronger the algorithm.
- The local and remote identity authentication methods.
 - To use the pre-shared key authentication method, you must determine the pre-shared key.
 - To use the RSA digital signature authentication method, you must determine the PKI domain for the local end to use. For information about PKI, see "[Configuring PKI](#)."

To configure IKEv2, perform the following tasks:

Tasks at a glance	Remarks
(Required.) Configuring an IKEv2 profile	N/A
(Required.) Configuring an IKEv2 policy	N/A
(Optional.) Configuring an IKEv2 proposal	If you specify an IKEv2 proposal in an IKEv2 policy, you must configure the IKEv2 proposal.
Configuring an IKEv2 keychain	Required when either end or both ends use the pre-shared key authentication method.
Configure global IKEv2 parameters • (Optional.) Enabling the cookie challenging feature • (Optional.) Configuring the IKEv2 DPD feature • (Optional.) Configuring the IKEv2 NAT keepalive feature • (Optional.) Configuring IKEv2 address pools	The cookie challenging feature takes effect only on IKEv2 responders.

Configuring an IKEv2 profile

An IKEv2 profile is intended to provide a set of parameters for IKEv2 negotiation. To configure an IKEv2 profile, perform the following tasks:

1. Specify the local and remote identity authentication methods.
The local and remote identity authentication methods must both be specified and they can be different. You can specify only one local identity authentication method and multiple remote identity authentication methods.
2. Configure the IKEv2 keychain or PKI domain for the IKEv2 profile to use:
 - To use digital signature authentication, configure a PKI domain.
 - To use pre-shared key authentication, configure an IKEv2 keychain.
3. Configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation:
 - For digital signature authentication, the device can use an ID of any type. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN as the local ID. The FQDN is the device name configured by using the **sysname** command.
 - For pre-shared key authentication, the device can use an ID of any type other than the DN.
4. Configure peer IDs.
The device compares the received peer ID with the peer IDs of its local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. IKEv2 profiles will be compared in descending order of their priorities.

5. Specify a local interface or IP address for the IKEv2 profile so the profile can be applied only to the specified interface or IP address. For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command). If no local address is configured, specify the IP address of the interface that uses the IPsec policy.
6. Specify a priority number for the IKEv2 profile. To determine the priority of an IKEv2 profile:
 - a. First, the device examines the existence of the **match local** command. An IKEv2 profile with the **match local** command configured has a higher priority.
 - b. If a tie exists, the device compares the priority numbers. An IKEv2 profile with a smaller priority number has a higher priority.
 - c. If a tie still exists, the device prefers an IKEv2 profile configured earlier.
7. Specify a VPN instance for the IKEv2 profile. The IKEv2 profile is used for IKEv2 negotiation only on the interfaces that belong to the VPN instance.
8. Configure the IKEv2 SA lifetime.
The local and remote ends can use different IKEv2 SA lifetimes. They do not negotiate the lifetime. The end with a smaller SA lifetime will initiate an SA negotiation when the lifetime expires.
9. Configure IKEv2 DPD to detect dead IKEv2 peers. You can also configure this feature in system view. If you configure IKEv2 DPD in both views, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.
10. Specify an inside VPN instance. This setting determines where the device should forward received IPsec packets after it de-encapsulates them. If you specify an inside VPN instance, the device looks for a route in the specified VPN instance to forward the packets. If you do not specify an inside VPN instance, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.
11. Configure the NAT keepalive interval.
Configure this task when the device is behind a NAT gateway. The device sends NAT keepalive packets regularly to its peer to prevent the NAT session from being aged because of no matching traffic.
12. Enable the configuration exchange feature.
The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response.
This feature typically applies to scenarios where branches and the headquarters communicate through virtual tunnels.
This feature enables the IPsec gateway at a branch to send IP address requests to the IPsec gateway at the headquarters. When the headquarters receives the request, it sends an IP address to the branch in the response packet. The headquarters can also actively push an IP address to the branch. The branch uses the allocated IP address as the IP address of the virtual tunnel to communicate with the headquarters.
13. Enable AAA authorization.
The AAA authorization feature enables IKEv2 to request authorization attributes, such as the IKEv2 address pool, from AAA. IKEv2 uses the address pool to assign IP addresses to remote users. For more information about AAA authorization, see "[Configuring AAA](#)."

To configure an IKEv2 profile:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 profile and enter IKEv2 profile view.	ikev2 profile <i>profile-name</i>	By default, no IKEv2 profiles exist.

Step	Command	Remarks
3. Configure the local and remote identity authentication methods.	authentication-method { local remote } { dsa-signature ecdsa-signature pre-share rsa-signature }	By default, no local or remote identity authentication method is configured.
4. Specify a keychain.	keychain <i>keychain-name</i>	By default, no keychain is specified for an IKEv2 profile. Perform this task when the pre-shared key authentication method is specified.
5. Specify a PKI domain.	certificate domain <i>domain-name</i> [sign verify]	By default, the device uses PKI domains configured in system view. Perform this task when the digital signature authentication method is specified.
6. Configure the local ID.	identity local { address { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } dn email <i>email-string</i> fqdn <i>fqdn-name</i> key-id <i>key-id-string</i> }	By default, no local ID is configured, and the device uses the IP address of the interface where the IPsec policy applies as the local ID.
7. Configure peer IDs.	match remote { certificate <i>policy-name</i> identity { address { { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] } range <i>low-ipv4-address</i> <i>high-ipv4-address</i> } ipv6 { <i>ipv6-address</i> [<i>prefix-length</i>] } range <i>low-ipv6-address</i> <i>high-ipv6-address</i> } } fqdn <i>fqdn-name</i> email <i>email-string</i> key-id <i>key-id-string</i> } }	By default, no peer ID is configured. You must configure a minimum of one peer ID on each of the two peers.
8. (Optional.) Specify the local interface or IP address to which the IKEv2 profile can be applied.	match local address { <i>interface-type</i> <i>interface-number</i> { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } }	By default, an IKEv2 profile can be applied to any local interface or IP address.
9. (Optional.) Specify a priority for the IKEv2 profile.	priority <i>priority</i>	By default, the priority of an IKEv2 profile is 100.
10. (Optional.) Specify a VPN instance for the IKEv2 profile.	match vrf { name <i>vrf-name</i> any }	By default, an IKEv2 profile belongs to the public network.
11. (Optional.) Set the IKEv2 SA lifetime for the IKEv2 profile.	sa duration <i>seconds</i>	By default, the IKEv2 SA lifetime is 86400 seconds.
12. (Optional.) Configure the DPD feature for the IKEv2 profile.	dpd interval <i>interval</i> [retry <i>seconds</i>] { on-demand periodic }	By default, DPD is disabled for an IKEv2 profile. The global DPD settings in system view are used. If DPD is also disabled in system view, the device does not perform DPD.
13. (Optional.) Specify an inside VPN instance for the IKEv2 profile.	inside-vrf <i>vrf-name</i>	By default, no inside VPN instance is specified for an IKEv2 profile. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.

Step	Command	Remarks
14. (Optional.) Set the IKEv2 NAT keepalive interval.	nat-keepalive <i>seconds</i>	By default, the global IKEv2 NAT keepalive setting is used.
15. (Optional.) Enable the configuration exchange feature.	config-exchange { request set { accept send } }	By default, all configuration exchange options are disabled.
16. (Optional.) Enable AAA authorization.	aaa authorization domain <i>domain-name</i> username <i>user-name</i>	By default, AAA authorization is disabled for IKEv2.

Configuring an IKEv2 policy

During the IKE_SA_INIT exchange, each end tries to find a matching IKEv2 policy, using the IP address of the local security gateway as the matching criterion.

- If IKEv2 policies are configured, IKEv2 searches for an IKEv2 policy that uses the IP address of the local security gateway. If no IKEv2 policy uses the IP address or the policy is using an incomplete proposal, the IKE_SA_INIT exchange fails.
- If no IKEv2 policy is configured, IKEv2 uses the system default IKEv2 policy **default**.

The device matches IKEv2 policies in the descending order of their priorities. To determine the priority of an IKEv2 policy:

1. First, the device examines the existence of the **match local address** command. An IKEv2 policy with the **match local address** command configured has a higher priority.
2. If a tie exists, the device compares the priority numbers. An IKEv2 policy with a smaller priority number has a higher priority.
3. If a tie still exists, the device prefers an IKEv2 policy configured earlier.

To configure an IKEv2 policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 policy and enter IKEv2 policy view.	ikev2 policy <i>policy-name</i>	By default, an IKEv2 policy named default exists.
3. Specify the local interface or address used for IKEv2 policy matching.	match local address { <i>interface-type interface-number</i> { { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } } }	By default, no local interface or address is used for IKEv2 policy matching, and the policy matches any local interface or address.
4. Specify a VPN instance for IKEv2 policy matching.	match vrf { name <i>vrf-name</i> any }	By default, no VPN instance is specified for IKEv2 policy matching. The IKEv2 policy matches all local addresses in the public network.
5. Specify an IKEv2 proposal for the IKEv2 policy.	proposal <i>proposal-name</i>	By default, no IKEv2 proposal is specified for an IKEv2 policy.
6. Specify a priority for the IKEv2 policy.	priority <i>priority</i>	By default, the priority of an IKEv2 policy is 100.

Configuring an IKEv2 proposal

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. An algorithm specified earlier has a higher priority.

A complete IKEv2 proposal must have at least one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

To configure an IKEv2 proposal:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 proposal and enter IKEv2 proposal view.	ikev2 proposal <i>proposal-name</i>	By default, an IKEv2 proposal named default exists. In non-FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and 3DES. • Integrity protection algorithms HMAC-SHA1 and HMAC-MD5. • PRF algorithms HMAC-SHA1 and HMAC-MD5. • DH groups 2 and 5. In FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and AES-CTR-128. • Integrity protection algorithms HMAC-SHA1 and HMAC-SHA256. • PRF algorithms HMAC-SHA1 and HMAC-SHA256. • DH groups 14 and 19.
3. Specify the encryption algorithms.	In non-FIPS mode: <pre>encryption { 3des-cbc aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-ctr-128 aes-ctr-192 aes-ctr-256 camellia-cbc-128 camellia-cbc-192 camellia-cbc-256 des-cbc } *</pre> In FIPS mode: <pre>encryption { aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-ctr-128 aes-ctr-192 aes-ctr-256 } *</pre>	By default, an IKEv2 proposal does not have any encryption algorithms.

Step	Command	Remarks
4. Specify the integrity protection algorithms.	In non-FIPS mode: integrity { aes-xcbc-mac md5 sha1 sha256 sha384 sha512 } * In FIPS mode: integrity { sha1 sha256 sha384 sha512 } *	By default, an IKEv2 proposal does not have any integrity protection algorithms.
5. Specify the PRF algorithms.	In non-FIPS mode: prf { aes-xcbc-mac md5 sha1 sha256 sha384 sha512 } * In FIPS mode: prf { sha1 sha256 sha384 sha512 } *	By default, an IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.
6. Specify the DH groups.	In non-FIPS mode: dh { group1 group14 group2 group24 group5 group19 group20 } * In FIPS mode: dh { group14 group19 group20 } *	By default, an IKEv2 proposal does not have any DH groups.

Configuring an IKEv2 keychain

An IKEv2 keychain specifies the pre-shared keys used for IKEv2 negotiation.

An IKEv2 keychain can have multiple IKEv2 peers. Each peer has a symmetric pre-shared key or an asymmetric pre-shared key pair, and information for identifying the peer (such as the peer's host name, IP address or address range, or ID).

An IKEv2 negotiation initiator uses the peer host name or IP address/address range as the matching criterion to search for a peer. A responder uses the peer host IP address/address range or ID as the matching criterion to search for a peer.

To configure an IKEv2 keychain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 keychain and enter IKEv2 keychain view.	ikev2 keychain <i>keychain-name</i>	By default, no IKEv2 keychains exist.
3. Create an IKEv2 peer and enter IKEv2 peer view.	peer <i>name</i>	By default, no IKEv2 peers exist.

Step	Command	Remarks
4. Configure the information for identifying the IKEv2 peer.	- To configure a host name for the peer: hostname <i>host-name</i> - To configure a host IP address or address range for the peer: address { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] ipv6 <i>ipv6-address</i> [<i>prefix-length</i>] } - To configure an ID for the peer: identity { address { <i>ipv4-address</i> ipv6 { <i>ipv6-address</i> } } fqdn <i>fqdn-name</i> email <i>email-string</i> key-id <i>key-id-string</i> }	By default, no hostname, host IP address, address range, or identity information is configured for an IKEv2 peer. You must configure different IP addresses/address ranges for different peers.
5. Configure a pre-shared key for the peer.	pre-shared-key [local remote] { ciphertext plaintext } <i>string</i>	By default, an IKEv2 peer does not have a pre-shared key.

Configure global IKEv2 parameters

Enabling the cookie challenging feature

Enable cookie challenging on responders to protect them against DoS attacks that use a large number of source IP addresses to forge IKE_SA_INIT requests.

To enable cookie challenging:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable cookie challenging.	ikev2 cookie-challenge <i>number</i>	By default, IKEv2 cookie challenging is disabled..

Configuring the IKEv2 DPD feature

IKEv2 DPD detects dead IKEv2 peers in periodic or on-demand mode.

- **Periodic DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages at regular intervals.
- **On-demand DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages before sending data.
 - Before the device sends data, it identifies the time interval for which the last IPsec packet has been received from the peer. If the time interval exceeds the DPD interval, it sends a DPD message to the peer to detect its liveliness.
 - If the device has no data to send, it never sends DPD messages.

If you configure IKEv2 DPD in both IKEv2 profile view and system view, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

To configure global IKEv2 DPD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure global IKEv2 DPD.	ikev2 dpd interval <i>interval</i> [retry <i>seconds</i>] { on-demand periodic }	By default, global DPD is disabled.

Configuring the IKEv2 NAT keepalive feature

Configure this feature on the IKEv2 gateway behind the NAT device. The gateway then sends NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

This feature takes effect after the device detects the NAT device.

To configure the IKEv2 NAT keepalive feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the IKEv2 NAT keepalive interval.	ikev2 nat-keepalive <i>seconds</i>	By default, the IKEv2 NAT keepalive interval is 10 seconds.

Configuring IKEv2 address pools

To perform centralized management on remote users, an IPsec gateway can use an address pool to assign private IP addresses to remote users.

You must use an IKEv2 address pool together with AAA authorization by specifying the IKEv2 address pool as an AAA authorization attribute. For more information about AAA authorization, see "[Configuring AAA](#)."

To configure IKE address pools:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure an IKEv2 IPv4 address pool.	ikev2 address-group <i>group-name</i> <i>start-ipv4-address</i> <i>end-ipv4-address</i> [<i>mask</i> <i>mask-length</i>]	By default, no IKEv2 IPv4 address pool exists.
3. Configure an IKEv2 IPv6 address pool.	ikev2 ipv6-address-group <i>group-name</i> prefix <i>prefix/prefix-len</i> assign-len <i>assign-len</i>	By default, no IKEv2 IPv6 address pool exists.

Displaying and maintaining IKEv2

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the IKEv2 proposal configuration.	display ikev2 proposal [<i>name</i> default]

Task	Command
Display the IKEv2 policy configuration.	display ikev2 policy [<i>policy-name</i> default]
Display the IKEv2 profile configuration.	display ikev2 profile [<i>profile-name</i>]
Display the IKEv2 SA information.	display ikev2 sa [[{ local remote } { <i>ipv4-address</i> <i>ipv6 ipv6-address</i> }] [vpn-instance <i>vpn-instance-name</i>]] [verbose [tunnel <i>tunnel-id</i>]]
Delete IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.	reset ikev2 sa [[{ local remote } { <i>ipv4-address</i> <i>ipv6 ipv6-address</i> }] [vpn-instance <i>vpn-instance-name</i>]] [tunnel <i>tunnel-id</i>] [fast]

IKEv2 configuration examples

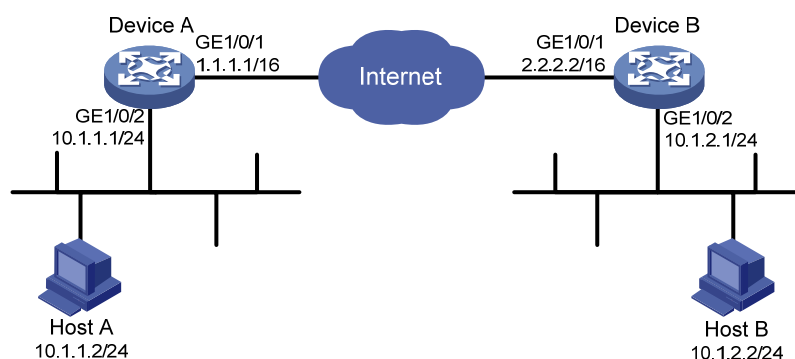
IKEv2 with pre-shared key authentication configuration example

Network requirements

As shown in [Figure 113](#), configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

- Configure Device A and Device B to use the default IKEv2 proposal and the default IKEv2 policy in IKEv2 negotiation to set up IPsec SAs.
- Configure the two devices to use the pre-shared key authentication method in IKEv2 negotiation.

Figure 113 Network diagram



Configuration procedures

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3101
```

```
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```

[DeviceA] ipsec transform-set tran1
# Set the packet encapsulation mode to tunnel.
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Use the ESP protocol for the IPsec transform set.
[DeviceA-ipsec-transform-set-tran1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
# Create an IKEv2 keychain named keychain1.
[DeviceA] ikev2 keychain keychain1
# Create an IKEv2 peer named peer1.
[DeviceA-ikev2-keychain-keychain1] peer peer1
# Specify the peer IP address 2.2.2.2/24.
[DeviceA-ikev2-keychain-keychain1-peer-peer1] address 2.2.2.2 24
# Specify the peer ID, which is the IP address 2.2.2.2.
[DeviceA-ikev2-keychain-keychain1-peer-peer1] identity address 2.2.2.2
# Specify the plaintext abcde as the pre-shared key to be used with the peer at 2.2.2.2.
[DeviceA-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext abcde
[DeviceA-ikev2-keychain-keychain1-peer-peer1] quit
[DeviceA-ikev2-keychain-keychain1] quit
# Create an IKEv2 profile named profile1.
[DeviceA] ikev2 profile profile1
# Specify the local authentication method as pre-shared key.
[DeviceA-ikev2-profile-profile1] authentication-method local pre-share
# Specify the remote authentication method as pre-shared key.
[DeviceA-ikev2-profile-profile1] authentication-method remote pre-share
# Specify the IKEv2 keychain keychain1.
[DeviceA-ikev2-profile-profile1] keychain keychain1
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the IP address 2.2.2.2/24.
[DeviceA-ikev2-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[DeviceA-ikev2-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
[DeviceA] ipsec policy map1 10 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# Specify the IPsec transform set tran1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# Specify the IKEv2 profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] ikev2-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 1/0/1.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1

```

```

[DeviceA-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host B resides.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
2. Configure Device B:
# Assign an IP address to each interface. (Details not shown.)
# Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.2.0/24 to subnet
10.1.1.0/24.
<DeviceB> system-view
[DeviceB] acl advanced 3101
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3101] quit
# Create an IPsec transform set named tran1.
[DeviceB] ipsec transform-set tran1
# Set the packet encapsulation mode to tunnel.
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-tran1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
# Create an IKEv2 keychain named keychain1.
[DeviceB] ikev2 keychain keychain1
# Create an IKEv2 peer named peer1.
[DeviceB-ikev2-keychain-keychain1] peer peer1
# Specify the peer IP address 1.1.1.1/24.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] address 1.1.1.1 24
# Specify the peer ID, which is the IP address 1.1.1.1.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] identity address 1.1.1.1
# Specify the plaintext abcde as the pre-shared key to be used with the peer at 1.1.1.1.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext abcde
[DeviceB-ikev2-keychain-keychain1-peer-peer1] quit
[DeviceB-ikev2-keychain-keychain1] quit
# Create an IKEv2 profile named profile1.
[DeviceB] ikev2 profile profile1
# Specify the local authentication method as pre-shared key.
[DeviceB-ikev2-profile-profile1] authentication-method local pre-share
# Specify the remote authentication method as pre-shared key.
[DeviceB-ikev2-profile-profile1] authentication-method remote pre-share
# Specify the IKEv2 keychain keychain1.
[DeviceB-ikev2-profile-profile1] keychain keychain1
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the IP address 1.1.1.1/24.
[DeviceA-ikev2-profile-profile1] match remote identity address 1.1.1.1 255.255.255.0
[DeviceA-ikev2-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 10.
[DeviceB] ipsec policy use1 10 isakmp

```

```

# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[DeviceB-ipsec-policy-isakmp-use1-10] remote-address 1.1.1.1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceB-ipsec-policy-isakmp-use1-10] security acl 3101
# Specify the IPsec transform set tran1 for the IPsec policy.
[DeviceB-ipsec-policy-isakmp-use1-10] transform-set tran1
# # Specify the IKEv2 profile profile1 for the IPsec policy.
[DeviceB-ipsec-policy-isakmp-use1-10] ikev2-profile profile1
[DeviceB-ipsec-policy-isakmp-use1-10] quit
# Apply the IPsec policy use1 to interface GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy use1
[DeviceB-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host A resides.
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKEv2 negotiation. After IPsec SAs are successfully negotiated by IKEv2, traffic between the two subnets is IPsec protected.

Display the IKEv2 proposal and IKEv2 policy on Device A.

```

[DeviceA] display ikev2 proposal
IKEv2 proposal : default
  Encryption : 3DES-CBC AES-CBC-128
  Integrity : MD596 SHA96
  PRF : MD5 SHA1
  DH Group : Group2 Group5

```

[DeviceA] display ikev2 policy

```

IKEv2 policy : default
  Match VPN instance : any

```

Display the IKEv2 SA on Device A.

[DeviceA] display ikev2 sa

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	2.2.2.2/500	EST

Status:

IN-NEG0: Negotiating, EST: Establish, DEL:Deleting

Display the IPsec SAs on Device A.

[DeviceA] display ipsec sa

```

-----
Interface: GigabitEthernet1/0/1
-----

```

```

-----
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----

```

```

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1456
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2
Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: IP
dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: IP

[Inbound ESP SAs]
SPI: 3264152513 (0xc28f03c1)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: active

[Outbound ESP SAs]
SPI: 738451674 (0x2c03e0da)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: active

# Display the IKEv2 proposal, IKEv2 policy, IKEv2 SA and IPsec SAs on Device B.
[DeviceB] display ikev2 proposal
[DeviceB] display ikev2 policy
[DeviceB] display ikev2 sa
[DeviceB] display ipsec sa

```

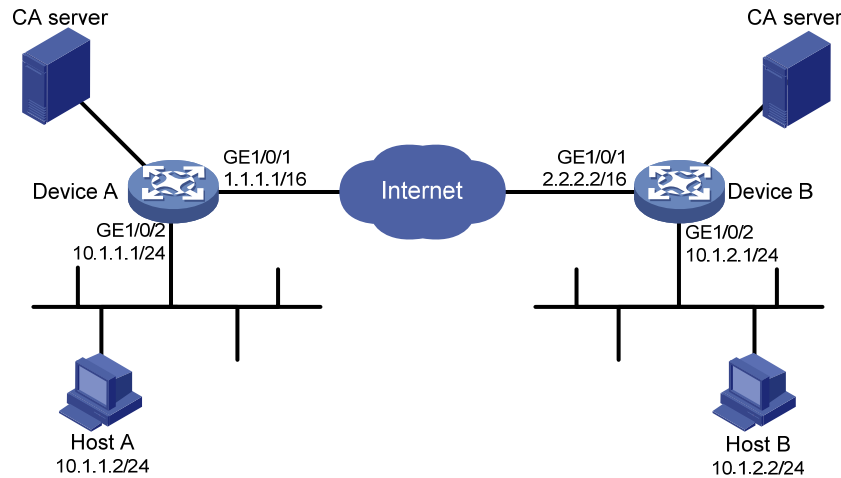
IKEv2 with RSA signature authentication configuration example

Network requirements

As shown in [Figure 114](#), configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

Configure Device A and Device B to use IKEv2 negotiation and RSA signature authentication. Device A acts as the initiator and the subnet where Device A resides uses IP addresses dynamically allocated.

Figure 114 Network diagram



Configuration procedure

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3101
```

```
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[DeviceA] ipsec transform-set tran1
```

Set the packet encapsulation mode to **tunnel**.

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Use the ESP protocol for the IPsec transform set.

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

Specify the encryption and authentication algorithms.

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
```

```
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[DeviceA-ipsec-transform-set-tran1] quit
```

Create a PKI entity named **entity1**.

```
[DeviceA] pki entity entity1
```

Set the common name to **routera** for the PKI entity.

```
[DeviceA-pki-entity-entity1] common-name routera
```

```
[DeviceA-pki-entity-entity1] quit
```

Create a PKI domain named **domain1**.

```
[DeviceA] pki domain domain1
```

Set the certificate request mode to **auto** and set the password to **123** for certificate revocation.

```
[DeviceA-pki-domain-domain1] certificate request mode auto password simple 123
```

Set an MD5 fingerprint for verifying the validity of the CA root certificate.

```
[DeviceA-pki-domain-domain1] root-certificate fingerprint md5 50c7a2d282ea710a449eede6c56b102e
```

```

# Specify the trusted CA 8088.
[DeviceA-pki-domain-domain1] ca identifier 8088
# Specify the URL of the registration server for certificate request through the SCEP protocol.
This example uses the URL of
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7.
[DeviceA-pki-domain-domain1] certificate request url
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7
# Specify the CA to accept certificate requests.
[DeviceA-pki-domain-domain1] certificate request from ca
# Specify the PKI entity for certificate request as entity1.
[DeviceA-pki-domain-domain1] certificate request entity entity1
# Specify the RSA key pair rsa1 with the general purpose for certificate request.
[DeviceA-pki-domain-domain1] public-key rsa general name rsa1
[DeviceA-pki-domain-domain1] quit
# Create an IKEv2 profile named profile1.
[DeviceA] ikev2 profile profile1
# Specify the local authentication method as RSA signatures.
[DeviceA-ikev2-profile-profile1] authentication-method local rsa-signature
# Specify the remote authentication method as RSA signatures.
[DeviceA-ikev2-profile-profile1] authentication-method remote rsa-signature
# Specify the PKI domain domain1 for the IKEv2 profile.
[DeviceA-ikev2-profile-profile1] certificate domain domain1
# Set the local ID to the FQDN name www.routera.com.
[DeviceA-ikev2-profile-profile1] identity local fqdn www.routera.com
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the FQDN name
www.routerb.com.
[DeviceA-ikev2-profile-profile1] match remote identity fqdn www.routerb.com
[DeviceA-ikev2-profile-profile1] quit
# Create an IKEv2 proposal named 10.
[DeviceA] ikev2 proposal 10
# Specify the integrity protection algorithm as HMAC-MD5.
[DeviceA-ikev2-proposal-10] integrity md5
# Specify the encryption algorithm as 3DES-CBC.
[DeviceA-ikev2-proposal-10] encryption 3des-cbc
# Specify the DH group as Group 1.
[DeviceA-ikev2-proposal-10] dh group1
# Specify the PRF algorithm as HMAC-MD5.
[DeviceA-ikev2-proposal-10] prf md5
[DeviceA-ikev2-proposal-10] quit
# Create an IKEv2 policy named 1.
[DeviceA] ikev2 policy 1
# Specify the IKEv2 proposal 10 for the IKEv2 policy.
[DeviceA-ikev2-policy-1] proposal 10
[DeviceA-ikev2-policy-1] quit
# Create an IKE-based IPsec policy entry with the name map1 and the sequence number 10.
[DeviceA] ipsec policy map1 10 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.

```

```
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# Specify the IPsec transform set tran1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# Specify the IKEv2 profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-map1-10] ikev2-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy map1 to interface GigabitEthernet 1/0/1.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host B resides.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```

2. Configure Device B:

```
# Assign an IP address to each interface. (Details not shown.)
# Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<DeviceB> system-view
[DeviceB] acl advanced 3101
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3101] quit
# Create an IPsec transform set named tran1.
[DeviceB] ipsec transform-set tran1
# Set the packet encapsulation mode to tunnel.
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-tran1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
# Create a PKI entity named entity2.
[DeviceB] pki entity entity2
# Set the common name to routerb for the PKI entity.
[DeviceB-pki-entity-entity2] common-name routerb
[DeviceB-pki-entity-entity2] quit
# Create a PKI domain named domain2.
[DeviceB] pki domain domain2
# Set the certificate request mode to auto and set the password to 123 for certificate revocation.
[DeviceB-pki-domain-domain2] certificate request mode auto password simple 123
# Set an MD5 fingerprint for verifying the validity of the CA root certificate.
[DeviceB-pki-domain-domain2] root-certificate fingerprint md5
50c7a2d282ea710a449eede6c56b102e
# Specify the trusted CA 8088.
[DeviceB-pki-domain-domain2] ca identifier 8088
```

```

# Specify the URL of the registration server for certificate request through the SCEP protocol.
This example uses the URL of
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7.
[DeviceB-pki-domain-domain2] certificate request url
http://192.168.222.1:446/eadb9af4f2c4641e685f7a6021e7b298373feb7
# Specify the CA to accept certificate requests.
[DeviceB-pki-domain-domain2] certificate request from ca
# Specify the PKI entity for certificate request as entity2.
[DeviceB-pki-domain-domain2] certificate request entity entity2
# Specify the RSA key pair rsa1 with the general purpose for certificate request.
[DeviceB-pki-domain-domain2] public-key rsa general name rsa1
[DeviceB-pki-domain-domain2] quit
# Create an IKEv2 profile named profile2.
[DeviceB] ikev2 profile profile2
# Specify the local authentication method as RSA signatures.
[DeviceB-ikev2-profile-profile2] authentication-method local rsa-signature
# Specify the remote authentication method as RSA signatures.
[DeviceB-ikev2-profile-profile2] authentication-method remote rsa-signature
# Set the local identity to the FQDN name www.routerb.com.
[DeviceB-ikev2-profile-profile2] identity local fqdn www.routerb.com
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the FQDN name
www.routera.com.
[DeviceB-ikev2-profile-profile2] match remote identity fqdn www.routera.com
[DeviceB-ikev2-profile-profile2] quit
# Create an IKEv2 proposal named 10.
[DeviceB] ikev2 proposal 10
# Specify the integrity protection algorithm as HMAC-MD5.
[DeviceB-ikev2-proposal-10] integrity md5
# Specify the encryption algorithm as 3DES-CBC.
[DeviceB-ikev2-proposal-10] encryption 3des-cbc
# Specify the DH group as Group 1.
[DeviceB-ikev2-proposal-10] dh group1
# Specify the PRF algorithm as HMAC-MD5.
[DeviceB-ikev2-proposal-10] prf md5
[DeviceB-ikev2-proposal-10] quit
# Create an IKEv2 policy named 1.
[DeviceB] ikev2 policy 1
# Specify the IKEv2 proposal 10 for the IKEv2 policy.
[DeviceB-ikev2-policy-1] proposal 10
[DeviceB-ikev2-policy-1] quit
# Create an IPsec policy template entry with the name template1 and the sequence number 1.
[DeviceB] ipsec policy-template template1 1
# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[DeviceB-ipsec-policy-template-template1-1] remote-address 1.1.1.1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceB-ipsec-policy-template-template1-1] security acl 3101
# Specify the IPsec transform set tran1 for the IPsec policy template.

```

```

[DeviceB-ipsec-policy-template-template1-1] transform-set tran1
# Specify the IKEv2 profile profile2 for the IPsec policy template.
[DeviceB-ipsec-policy-template-template1-1] ikev2-profile profile2
[DeviceB-ipsec-policy-template-template1-1] quit
# Create an IKE-based IPsec policy entry with the name use1 and the sequence number 1 by
using the IPsec policy template template1.
[DeviceB] ipsec policy use1 1 isakmp template template1
# Apply IPsec policy use1 to interface GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy use1
[DeviceB-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host A resides.
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKEv2 negotiation. After IPsec SAs are successfully negotiated by IKEv2, traffic between the two subnets is IPsec protected.

Display the IKEv2 proposal configuration on Device A and Device B.

```
[DeviceA] display ikev2 proposal 10
```

```

IKEv2 proposal : 10
  Encryption : 3DES-CBC
  Integrity : MD596
  PRF : MD5
  DH Group : Group1

```

```
[DeviceB] display ikev2 proposal 10
```

```

IKEv2 proposal : 10
  Encryption : 3DES-CBC
  Integrity : MD596
  PRF : MD5
  DH Group : Group1

```

Display the IKEv2 policy configuration Device A and Device B.

```
[DeviceA] display ikev2 policy 1
```

```

IKEv2 policy : 1
  Match Local : any
  Match VPN instance : public
  Proposal : 1

```

```
[DeviceB] display ikev2 policy 1
```

```

IKEv2 policy : 1
  Match Local : any
  Match VPN instance : public
  Proposal : 1

```

Display the IKEv2 SA on Device A.

```
[DeviceA] display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	2.2.2.2/500	EST

Status:

IN-NEG0: Negotiating, EST: Establish, DEL:Deleting
Display information about the CA certificate on Device A.
[DeviceA] display pki certificate domain domain1 ca
Certificate:

Data:

Version: 1 (0x0)
Serial Number:
b9:14:fb:25:c9:08:2c:9d:f6:94:20:30:37:4e:00:00
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=cn, O=rnd, OU=sec, CN=8088
Validity
Not Before: Sep 6 01:53:58 2012 GMT
Not After : Sep 8 01:50:58 2015 GMT
Subject: C=cn, O=rnd, OU=sec, CN=8088
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:de:81:f4:42:c6:9f:c2:37:7b:21:84:57:d6:42:
00:69:1c:4c:34:a4:5e:bb:30:97:45:2b:5e:52:43:
c0:49:1f:e1:d8:0f:5c:48:c2:39:69:d1:84:e4:14:
70:3d:98:41:28:1c:20:a1:9a:3f:91:67:78:77:27:
d9:08:5f:7a:c4:36:45:8b:f9:7b:e7:7d:6a:98:bb:
4e:a1:cb:2c:3d:92:66:bd:fb:80:35:16:c6:35:f0:
ff:0b:b9:3c:f3:09:94:b7:d3:6f:50:8d:83:f1:66:
2f:91:0b:77:a5:98:22:b4:77:ac:84:1d:03:8e:33:
1b:31:03:78:4f:77:a0:db:af
Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
9a:6d:8c:46:d3:18:8a:00:ce:12:ee:2b:b0:aa:39:5d:3f:90:
08:49:b9:a9:8f:0d:6e:7b:e1:00:fb:41:f5:d4:0c:e4:56:d8:
7a:a7:61:1d:2b:b6:72:e3:09:0b:13:9d:fa:c8:fc:c4:65:a7:
f9:45:21:05:75:2c:bf:36:7b:48:b4:4a:b9:fe:87:b9:d8:cf:
55:16:87:ec:07:1d:55:5a:89:74:73:68:5e:f9:1d:30:55:d9:
8a:8f:c5:d4:20:7e:41:a9:37:57:ed:8e:83:a7:80:2f:b8:31:
57:3a:f2:1a:28:32:ea:ea:c5:9a:55:61:6a:bc:e5:6b:59:0d:
82:16

Display the local certificate on Device A.
[DeviceA]display pki certificate domain domain1 local
Certificate:

Data:

Version: 3 (0x2)
Serial Number:
a1:f4:d4:fd:cc:54:c3:07:c4:9e:15:2d:5f:64:57:77
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=cn, O=rnd, OU=sec, CN=8088
Validity
Not Before: Sep 26 02:06:43 2012 GMT

Not After : Sep 26 02:06:43 2013 GMT
Subject: CN=devicea
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:b0:a1:cd:24:6e:1a:1d:51:79:f0:2a:3e:9f:e9:
84:07:16:78:49:1b:7d:0b:22:f0:0a:ed:75:91:a4:
17:fd:c7:ef:d0:66:5c:aa:e3:2a:d9:71:12:e4:c6:
25:77:f0:1d:97:bb:92:a8:bd:66:f8:f8:e8:d5:0d:
d2:c8:01:dd:ea:e6:e0:80:ad:db:9d:c8:d9:5f:03:
2d:22:07:e3:ed:cc:88:1e:3f:0c:5e:b3:d8:0e:2d:
ea:d6:c6:47:23:6a:11:ef:3c:0f:6b:61:f0:ca:a1:
79:a0:b1:02:1a:ae:8c:c9:44:e0:cf:d1:30:de:4c:
f0:e5:62:e7:d0:81:5d:de:d3
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 CRL Distribution Points:

Full Name:
URI:http://xx.rsa.com:447/8088.crl

Signature Algorithm: sha1WithRSAEncryption
73:ac:66:f9:b8:b5:39:e1:6a:17:e4:d0:72:3e:26:9e:12:61:
9e:c9:7a:86:6f:27:b0:b9:a3:5d:02:d9:5a:cb:79:0a:12:2e:
cb:e7:24:57:e6:d9:77:12:6b:7a:cf:ee:d6:17:c5:5f:d2:98:
30:e0:ef:00:39:4a:da:ff:1c:29:bb:2a:5b:60:e9:33:8f:78:
f9:15:dc:a5:a3:09:66:32:ce:36:cd:f0:fe:2f:67:e5:72:e5:
21:62:85:c4:07:92:c8:f1:d3:13:9c:2e:42:c1:5f:0e:8f:ff:
65:fb:de:7c:ed:53:ab:14:7a:cf:69:f2:42:a4:44:7c:6e:90:
7e:cd

Display the IPsec SAs on Device A.

[DeviceA] display ipsec sa

Interface: GigabitEthernet1/0/1

IPsec policy: map1
Sequence number: 10
Mode: ISAKMP

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1456
Tunnel:
local address: 1.1.1.1

```

        remote address: 2.2.2.2
Flow:
sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: ip

[Inbound ESP SAs]
  SPI: 3264152513 (0xc28f03c1)
  Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843200/3484
  Max received sequence-number:
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for NAT traversal: N
  Status: active

[Outbound ESP SAs]
  SPI: 738451674 (0x2c03e0da)
  Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843200/3484
  Max received sequence-number:
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for NAT traversal: N
  Status: active

# Display the information about the CA certificate, local certificate, IKEv2 SA, and IPsec SA on
Device B.
[DeviceB] display ikev2 sa
[DeviceB] display pki certificate domain domain2 ca
[DeviceB] display pki certificate domain domain2 local
[DeviceB] display ipsec sa

```

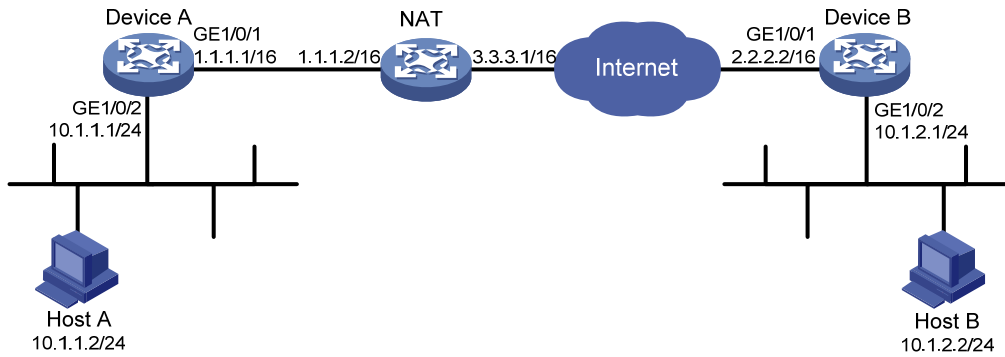
IKEv2 with NAT traversal configuration example

Network requirements

As shown in [Figure 115](#), Device A is behind the NAT device. Configure an IKE-based IPsec tunnel between Device A and Device B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

- Configure Device A and Device B to use the default IKEv2 proposal and the default IKEv2 policy in IKEv2 negotiation to set up IPsec SAs.
- Configure the two devices to use the pre-shared key authentication method in IKEv2 negotiation.

Figure 115 Network diagram



Configuration procedure

1. Configure Device A:

Assign an IP address to each interface. (Details not shown.)

Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
<DeviceA> system-view
```

```
[DeviceA] acl advanced 3101
```

```
[DeviceA-acl-ipv4-adv-3101] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

```
[DeviceA-acl-ipv4-adv-3101] quit
```

Create an IPsec transform set named **transform1**.

```
[DeviceA] ipsec transform-set transform1
```

Use the ESP protocol for the IPsec transform set.

```
[DeviceA-ipsec-transform-set-transform1] protocol esp
```

Specify the encryption and authentication algorithms.

```
[DeviceA-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
```

```
[DeviceA-ipsec-transform-set-transform1] esp authentication-algorithm md5
```

```
[DeviceA-ipsec-transform-set-transform1] quit
```

Create an IKEv2 keychain named **keychain1**.

```
[DeviceA] ikev2 keychain keychain1
```

Create an IKEv2 peer named **peer1**.

```
[DeviceA-ikev2-keychain-keychain1] peer peer1
```

Specify the peer IP address 2.2.2.2/24.

```
[DeviceA-ikev2-keychain-keychain1-peer-peer1] address 2.2.2.2 24
```

Specify the peer ID, which is the IP address 2.2.2.2.

```
[DeviceA-ikev2-keychain-keychain1-peer-peer1] identity address 2.2.2.2
```

Specify the plaintext **123** as the pre-shared key to be used with the peer.

```
[DeviceA-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext 123
```

```
[DeviceA-ikev2-keychain-keychain1-peer-peer1] quit
```

```
[DeviceA-ikev2-keychain-keychain1] quit
```

Create an IKEv2 profile named **profile1**.

```
[DeviceA] ikev2 profile profile1
```

Specify the IKEv2 keychain **keychain1**.

```
[DeviceA-ikev2-profile-profile1] keychain keychain1
```

Set the local ID to the FQDN name **www.devicea.com**.

```

[DeviceA-ikev2-profile-profile1] identity local fqdn www.devicea.com
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the IP address 2.2.2.2/24.
[DeviceA-ikev2-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[DeviceA-ikev2-profile-profile1] quit
# Create an IKE-based IPsec policy entry with the name policy1 and the sequence number 1.
[DeviceA] ipsec policy policy1 1 isakmp
# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 2.2.2.2
# Specify the IPsec transform set transform1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set transform1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3101
# Specify the IKEv2 profile profile1 for the IPsec policy.
[DeviceA-ipsec-policy-isakmp-policy1-1] ikev2-profile profile1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
# Apply the IPsec policy policy1 to interface GigabitEthernet 1/0/1.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host B resides.
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2

```

2. Configure Device B:

```

# Assign an IP address to each interface. (Details not shown.)
# Configure IPv4 advanced ACL 3101 to identify traffic from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<DeviceA> system-view
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
# Create an IPsec transform set named transform1.
<DeviceB> system-view
[DeviceB] ipsec transform-set transform1
# Use the ESP protocol for the IPsec transform set.
[DeviceB-ipsec-transform-set-transform1] protocol esp
# Specify the encryption and authentication algorithms.
[DeviceB-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
[DeviceB-ipsec-transform-set-transform1] esp authentication-algorithm md5
[DeviceB-ipsec-transform-set-transform1] quit
# Create an IKEv2 keychain named keychain1.
[DeviceB] ikev2 keychain keychain1
# Create an IKEv2 peer named peer1.
[DeviceB-ikev2-keychain-keychain1] peer peer1
# Specify the peer IP address 1.1.1.1/24.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] address 1.1.1.1 24
# Specify the peer ID, which is the IP address 1.1.1.1.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] identity address 1.1.1.1

```

```

# Specify the plaintext 123 as the pre-shared key to be used with the peer.
[DeviceB-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext 123
[DeviceB-ikev2-keychain-keychain1-peer-peer1] quit
[DeviceB-ikev2-keychain-keychain1] quit
# Create an IKEv2 profile named profile1.
[DeviceB] ikev2 profile profile1
# Specify the IKEv2 keychain keychain1.
[DeviceB-ikev2-profile-profile1] keychain keychain1
# Specify the peer ID that the IKEv2 profile matches. The peer ID is the FQDN name
www.devicea.com.
[DeviceB-ikev2-profile-profile1] match remote identity fqdn www.devicea.com
[DeviceB-ikev2-profile-profile1] quit
# Create an IPsec policy template entry with the name template1 and the sequence number 1.
[DeviceB] ipsec policy-template template1 1
# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[DeviceB-ipsec-policy-template-template1-1] remote-address 1.1.1.1
# Specify ACL 3101 to identify the traffic to be protected.
[DeviceB-ipsec-policy-template-template1-1] security acl 3101
# Specify the IPsec transform set transform1 for the IPsec policy template.
[DeviceB-ipsec-policy-template-template1-1] transform-set transform1
# Specify the IKEv2 profile profile1 for the IPsec policy template.
[DeviceB-ipsec-policy-template-template1-1] ikev2-profile profile1
[DeviceB-ipsec-policy-template-template1-1] quit
# Create an IKE-based IPsec policy entry with the name policy1 and the sequence number 1
by using the IPsec policy template template1.
[DeviceB] ipsec policy policy1 1 isakmp template template1
# Apply the IPsec policy policy1 to interface GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy policy1
[DeviceB-GigabitEthernet1/0/1] quit
# Configure a static route to the subnet where Host A resides. The next hop is the IP address of
the output interface on the NAT device. (Details not shown.)

```

Verifying the configuration

Initiate a connection from subnet 10.1.1.0/24 to subnet 10.1.2.0/24 to trigger IKEv2 negotiation. After IPsec SAs are successfully negotiated by IKEv2, traffic between the two subnets is IPsec protected.

Display the IKEv2 SA on Device A.

```
[DeviceA] display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	2.2.2.2/500	EST

Status:

IN-NEG0: Negotiating, EST: Establish, DEL:Deleting

```
[DeviceA] display ikev2 sa verbose
```

```
-----
Connection ID: 13
```

```
Outside VPN:
```

```

Inside VPN:
Profile: profile1
Transmitting entity: Initiator
-----
Local IP: 1.1.1.1
Local ID type: FQDN
Local ID: www.devicea.com

Remote IP: 2.2.2.2
Remote ID type: IPV4_ADDR
Remote ID: 2.2.2.2

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400
Remaining key duration(sec): 84565
Exchange-mode: Aggressive
Diffie-Hellman group: Group 1
NAT traversal: Detected

# Display the IPsec SAs on Device A.
[DeviceA] display ipsec sa
-----
Interface: GigabitEthernet1/0/1
-----

-----
IPsec policy: policy1
Sequence number: 1
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1435
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2

Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: IP
dest addr: 10.2.1.0/255.255.255.0 port: 0 protocol: IP

[Inbound ESP SAs]
SPI: 830667426 (0x3182faa2)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/2313

```

Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for nat traversal: Y
Status: active

[Outbound ESP SAs]

SPI: 3516214669 (0xd1952d8d)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/2313
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for nat traversal: Y
Status: active

Troubleshooting IKEv2

IKEv2 negotiation failed because no matching IKEv2 proposals were found

Symptom

The IKEv2 SA is in IN-NEGO status.

<Sysname> display ikev2 sa

Tunnel ID	Local	Remote	Status
5	123.234.234.124/500	123.234.234.123/500	IN-NEGO

Status:

IN-NEGO: Negotiating, EST: Establish, DEL:Deleting

Analysis

Certain IKEv2 proposal settings are incorrect.

Solution

1. Examine the IKEv2 proposal configuration to see whether the two ends have matching IKEv2 proposals.
2. Modify the IKEv2 proposal configuration to make sure the two ends have matching IKEv2 proposals.

IPsec SA negotiation failed because no matching IPsec transform sets were found

Symptom

The **display ikev2 sa** command shows that the IKEv2 SA negotiation succeeded and the IKEv2 SA is in EST status. The **display ipsec sa** command shows that the expected IPsec SAs have not been negotiated yet.

Analysis

Certain IPsec policy settings are incorrect.

Solution

1. Examine the IPsec configuration to see whether the two ends have matching IPsec transform sets.
2. Modify the IPsec configuration to make sure the two ends have matching IPsec transform sets.

IPsec tunnel establishment failed

Symptom

The ACLs and IKEv2 proposals are correctly configured on both ends. The two ends cannot establish an IPsec tunnel or cannot communicate through the established IPsec tunnel.

Analysis

The IKEv2 SA or IPsec SAs on either end are lost. The reason might be that the network is unstable and the device reboots.

Solution

1. Use the **display ikev2 sa** command to examine whether an IKEv2 SA exists on both ends. If the IKEv2 SA on one end is lost, delete the IKEv2 SA on the other end by using the **reset ikev2 sa** command and trigger new negotiation. If an IKEv2 SA exists on both ends, go to the next step.
2. Use the **display ipsec sa** command to examine whether IPsec SAs exist on both ends. If the IPsec SAs on one end are lost, delete the IPsec SAs on the other end by using the **reset ipsec sa** command and trigger new negotiation.

Configuring SSH

Overview

Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.

SSH uses the typical client-server model to establish a channel for secure data transfer based on TCP.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 is better than SSH1 in performance and security.

The device supports the following SSH applications:

- **Secure Telnet**—Stelnet provides secure and reliable network terminal access services. Through Stelnet, a user can securely log in to a remote server. Stelnet can protect devices against attacks, such as IP spoofing and plain text password interception. The device can act as an Stelnet server or an Stelnet client.
- **Secure File Transfer Protocol**—Based on SSH2, SFTP uses SSH connections to provide secure file transfer. The device can act as an SFTP server, allowing a remote user to log in to the SFTP server for secure file management and transfer. The device can also act as an SFTP client, enabling a user to log in from the device to a remote device for secure file transfer.
- **Secure Copy**—Based on SSH2, SCP offers a secure method to copy files. The device can act as an SCP server, allowing a user to log in to the device for file upload and download. The device can also act as an SCP client, enabling a user to log in from the device to a remote device for secure file transfer.
- **NETCONF over SSH**—Based on SSH2, it enables users to securely log in to the device through SSH and perform NETCONF operations on the device through the NETCONF-over-SSH connections. The device can act only as a NETCONF-over-SSH server. For more information about NETCONF, see *Network Management and Monitoring Configuration Guide*.

When acting as an SSH client or server, the device supports the following SSH versions:

- When acting as an SSH client, the device supports only SSH2.
- When acting as an Stelnet, SFTP, or SCP server, the device supports both SSH2 and SSH1 in non-FIPS mode and only SSH2 in FIPS mode.
- When acting as a NETCONF-over-SSH server, the device supports only SSH2 in either non-FIPS mode or FIPS modes.

How SSH works

This section uses SSH2 as an example to describe the stages to establish an SSH session. For more information about these stages, see *SSH Technology White Paper*.

Table 12 Stages to establish an SSH session

Stages	Description
Connection establishment	The SSH server listens to connection requests on port 22. After a client initiates a connection request, the server and the client establish a TCP connection.
Version negotiation	The two parties determine a version to use.

Stages	Description
Algorithm negotiation	SSH supports multiple algorithms. Based on the local algorithms, the two parties negotiate the following algorithms: • Key exchange algorithm for generating session keys. • Encryption algorithm for encrypting data. • Public key algorithm for digital signature and authentication. • HMAC algorithm for protecting data integrity.
Key exchange	The two parties use the DH exchange algorithm to dynamically generate the session keys and session ID. • The session keys are used for protecting data transfer. • The session ID is used for identifying the SSH connection. In this stage, the client also authenticates the server.
Authentication	The SSH server authenticates the client in response to the client's authentication request.
Session request	After passing the authentication, the client sends a session request to the server to request the establishment of a session (or request the Stelnet, SFTP, SCP, or NETCONF service).
Interaction	After the server grants the request, the client and the server start to communicate with each other in the session. In this stage, you can paste commands in text format and execute them at the CLI. The text pasted at one time must be no more than 2000 bytes. As a best practice to ensure the correct execution of commands, paste commands that are in the same view. To execute commands of more than 2000 bytes, save the commands in a configuration file, upload the file to the server through SFTP, and use it to restart the server.

SSH authentication methods

This section describes authentication methods that are supported by the device when it acts as an SSH server.

Password authentication

The SSH server authenticates a client through the AAA mechanism. The password authentication process is as follows:

1. The client sends the server an authentication request that includes the encrypted username and password.
2. The server performs the following operations:
 - a. Decrypts the request to get the username and password in plain text.
 - b. Verifies the username and password locally or through remote AAA authentication.
 - c. Informs the client of the authentication result.

If the remote AAA server requires the user to enter a password for secondary authentication, it send the SSH server an authentication response carrying a prompt. The prompt is transparently transmitted to the client to notify the user to enter a specific password. When the user enters the correct password, the AAA sever examines the password validity. If the password is valid, the SSH server returns an authentication success message to the client.

For more information about AAA, see "[Configuring AAA](#)."

NOTE:

SSH1 clients do not support secondary password authentication that is initiated by the AAA server.

Publickey authentication

The server authenticates a client by verifying the digital signature of the client. The publickey authentication process is as follows:

1. The client sends the server a publickey authentication request that includes the username, public key, and public key algorithm name.
If the digital certificate of the client is required in authentication, the client also encapsulates the digital certificate in the authentication request. The digital certificate carries the public key information of the client.
2. The server verifies the client's public key.
 - If the public key is invalid, the server informs the client of the authentication failure.
 - If the public key is valid, the server requests the digital signature of the client. After receiving the signature, the server uses the public key to verify the signature and informs the client of the authentication result.

When acting as an SSH server, the device supports using the public key algorithms RSA and DSA to verify digital signatures.

When acting as an SSH client, the device supports using the public key algorithms RSA and DSA to generate digital signatures.

For more information about public key configuration, see "[Managing public keys](#)."

Password-publickey authentication

The server requires SSH2 clients to pass both password authentication and publickey authentication. However, an SSH1 client only needs to pass either authentication.

Any authentication

The server requires clients to pass password authentication or publickey authentication.

SSH support for Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. [Table 13](#) lists all algorithms in Suite B.

The SSH server and client support using the X.509v3 certificate for identity authentication in compliance with the algorithm, negotiation, and authentication specifications defined in RFC 6239.

Table 13 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AEAD_AES_128_GCM AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Protocols and standards

RFC 6239, *Suite B Cryptographic Suites for Secure Shell (SSH)*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see "[Configuring FIPS](#)."

Configuring the device as an SSH server

SSH server configuration task list

Tasks at a glance	Remarks
(Optional.) Generating local DSA or RSA key pairs	N/A
(Required.) Enabling the Stelnet server	Required only for Stelnet servers.
(Required.) Enabling the SFTP server	Required only for SFTP servers.
(Required.) Enabling the SCP server	Required only for SCP servers.
(Required.) Enabling NETCONF over SSH	Required only for NETCONF-over-SSH servers.
(Required.) Configuring the user lines for SSH login	Required only for Stelnet and NETCONF-over-SSH servers.
(Required.) Configuring a client's host public key	Required if the authentication method is publickey , password-publickey , or any .
Configuring the PKI domain for verifying the client's digital certificate	See " Configuring PKI ." Required if the following conditions exist: The authentication method is publickey . The client sends its public key to the server through a digital certificate for validity check. The PKI domain must have the CA certificate to verify the client's digital certificate.
(Required/optional.) Configuring an SSH user	Required if the authentication method is publickey , password-publickey , or any . Optional if the authentication method is password .
(Optional.) Configuring the SSH management parameters	N/A
(Optional.) Specifying a PKI domain for the SSH server	N/A

Generating local DSA or RSA key pairs

The DSA or RSA key pairs on the SSH server are required for generating the session keys and session ID in the key exchange stage. They can also be used by a client to authenticate the server. When a client authenticates the server, it compares the public key received from the server with the server's public key that the client saved locally. If the keys are consistent, the client uses the locally saved server's public key to decrypt the digital signature received from the server. If the decryption succeeds, the server passes the authentication.

The SSH application starts when you execute an SSH server command on the device. If the device does not have RSA key pairs with default names, the device automatically generates one RSA server key pair and one RSA host key pair. Both key pairs use their default names.

You can also use the **public-key local create** command to generate DSA or RSA key pairs on the device.

Configuration restrictions and guidelines

When you generate local DSA or RSA key pairs, follow these restrictions and guidelines:

- SSH supports locally generated DSA and RSA key pairs only with default names.
- To support SSH clients that use different types of key pairs, generate both DSA and RSA key pairs on the SSH server.
- The SSH server operating in FIPS mode supports only RSA key pairs. Do not generate local DSA key pairs when the device operates as an SSH server in FIPS mode.
- The **public-key local create rsa** command generates a server key pair and a host key pair for RSA. In SSH1, the public key in the server key pair is used to encrypt the session key for secure transmission of the session key. Because SSH2 uses the DH algorithm to separately generate each session key on the SSH server and the client, no session key transmission is required. The server key pair is not used in SSH2.
- The **public-key local create dsa** command generates only a host key pair. SSH1 does not support the DSA algorithm.
- The key modulus length must be less than 2048 bits when you generate the DSA key pair on the SSH server.

Configuration procedure

To generate local DSA or RSA key pairs on the SSH server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Generate local DSA or RSA key pairs.	public-key local create { dsa rsa }	By default, no DSA or RSA key pairs exist on the server.

Enabling the Stelnet server

After you enable the Stelnet server on the device, a client can log in to the device through Stelnet.

To enable the Stelnet server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the Stelnet server.	ssh server enable	By default, the Stelnet server is disabled.

Enabling the SFTP server

After you enable the SFTP server on the device, a client can log in to the device through SFTP.

When acting as an SFTP server, the device does not support SFTP connections initiated by SSH1 clients.

To enable the SFTP server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enable the SFTP server.	sftp server enable	By default, the SFTP server is disabled.

Enabling the SCP server

After you enable the SCP server on the device, a client can log in to the device through SCP.

When acting as an SCP server, the device does not support SCP connections initiated by SSH1 clients.

To enable the SCP server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SCP server.	scp server enable	By default, the SCP server is disabled.

Enabling NETCONF over SSH

After you enable NETCONF over SSH on the device, a client can perform NETCONF operations on the device through a NETCONF-over-SSH connection.

When acting as a server in the NETCONF-over-SSH connection, the device does not support connection requests initiated by SSH1 clients.

To enable NETCONF over SSH:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Enable NETCONF over SSH.	netconf ssh server enable	By default, NETCONF over SSH is disabled. For more information about NETCONF over SSH commands, see <i>Network Management and Monitoring Command Reference</i> .

Configuring the user lines for SSH login

Depending on the SSH application, an SSH client can be an Stelnet client, SFTP client, SCP client, or NETCONF-over-SSH client.

Only Stelnet and NETCONF-over-SSH clients require the user line configuration. The user line configuration takes effect on the clients at the next login.

To configure the user lines for Stelnet and NETCONF-over-SSH clients:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VTY user line view.	line vty number [ending-number]	N/A

Step	Command	Remarks
3. Set the login authentication mode to scheme .	authentication-mode scheme	By default, the authentication mode is password . For more information about this command, see <i>Fundamentals Command Reference</i> .

Configuring a client's host public key

In publickey authentication, the server compares the SSH username and the client's host public key received from the client with the locally saved SSH username and the client's host public key. If they are the same, the server checks the digital signature that the client sends. The client generates the digital signature by using the private key that is paired with the client's host public key.

For publickey authentication, password-publickey authentication, or any authentication, you must perform the following tasks:

1. Configure the client's DSA or RSA host public key on the server.
As a best practice, configure no more than 20 SSH client's host public keys on an SSH server.
2. Specify the associated host private key on the client to generate the digital signature.
If the device acts as an SSH client, specify the public key algorithm on the client. The algorithm determines the associated host private key for generating the digital signature.

You can enter the content of a client's host public key or import the client's host public key from the public key file. As a best practice, import the client's host public key.

Entering a client's host public key

Before you enter the client's host public key, you must use the **display public-key local public** command on the client to obtain the client's host public key.

To enter a client's host public key:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public key view.	public-key peer keyname	N/A
3. Configure a client's host public key.	Enter the content of the client's host public key	The host public key must be in the DER encoding format without being converted. When you enter the content of a client's host public key, you can use spaces and carriage returns between characters. When you save the host public key, spaces and carriage returns are removed automatically. For more information, see "Managing public keys."
4. Return to system view.	peer-public-key end	N/A

Importing a client's host public key from the public key file

Before you import the host public key, upload the client's public key file (in binary) to the server, for example, through FTP or TFTP. During the import process, the server automatically converts the host public key in the public key file to a string in PKCS format.

To import a client's host public key from the public key file:

Step	Command
1. Enter system view.	system-view
2. Import a client's public key from the public key file.	public-key peer <i>keyname</i> import <i>sshkey filename</i>

Configuring an SSH user

Configure an SSH user and a local user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.
- If the authentication method is **password**, you must perform one of the following tasks:
 - For local authentication, configure a local user on the SSH server.
 - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

You do not need to create an SSH user by using the **ssh user** command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.

- If the authentication method is **password-publickey** or **any**, you must create an SSH user on the SSH server and perform one of the following tasks:
 - For local authentication, configure a local user on the SSH server.
 - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

For information about configuring local users and remote authentication, see "[Configuring AAA](#)."

Configuration restrictions and guidelines

When you configure an SSH user, follow these restrictions and guidelines:

- An SSH server supports up to 1024 SSH users.
- For an SFTP or SCP user, the working directory depends on the authentication method.
 - If the authentication method is **password**, the working directory is authorized by AAA.
 - If the authentication method is **publickey** or **password-publickey**, the working folder is specified by the **authorization-attribute** command in the associated local user view.
- For an SSH user, the user role also depends on the authentication method.
 - If the authentication method is **password**, the user role is authorized by the remote AAA server or the local device.
 - If the authentication method is **publickey** or **password-publickey**, the user role is specified by the **authorization-attribute** command in the associated local user view.
- If you change the authentication parameters for a logged-in SSH user, the change takes effect on the user at the next login.
- For all authentication methods except password authentication, you must specify a client's host public key or digital certificate.
 - For a client that sends the user's public key information directly to the server, specify the client's host public key on the server. The specified public key must already exist. For more information about public keys, see "[Configuring a client's host public key](#)."

- For a client that sends the user's public key information to the server through a digital certificate, specify a PKI domain on the server to verify the client's digital certificate. For successful verification, the specified PKI domain must have the correct CA certificate. To specify the PKI domain, use the **ssh user** or **ssh server pki-domain** command. For more information about configuring a PKI domain, see "[Configuring PKI](#)."
- When the device operates as an SSH server in FIPS mode, the device does not support the authentication method of **any** or **publickey**.

Configuration procedure

To configure an SSH user, and specify the service type and authentication method:

Step	Command
1. Enter system view.	system-view
2. Create an SSH user, and specify the service type and authentication method.	- In non-FIPS mode: ssh user <i>username</i> service-type { all netconf scp sftp stelnet } authentication-type { password { any password-publickey publickey } [assign { pki-domain <i>domain-name</i> publickey <i>keyname</i> }] } - In FIPS mode: ssh user <i>username</i> service-type { all netconf scp sftp stelnet } authentication-type { password password-publickey [assign { pki-domain <i>domain-name</i> publickey <i>keyname</i> }] }

Configuring the SSH management parameters

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SSH server to support SSH1 clients.	ssh server compatible-ssh1x enable	By default, the SSH server does not support SSH1 clients. This command is not available in FIPS mode.
3. Set the minimum interval for updating the RSA server key pair.	ssh server rekey-interval <i>hours</i>	By default, the RSA server key pair is not updated. This command takes effect only on SSH1 users. This command is not available in FIPS mode.
4. Set the SSH user authentication timeout timer.	ssh server authentication-timeout <i>time-out-value</i>	The default setting is 60 seconds. If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.
5. Set the maximum number of SSH authentication attempts.	ssh server authentication-retries <i>times</i>	The default setting is 3. If the authentication method is any , the total number of publickey authentication attempts and password authentication attempts cannot exceed the upper limit.

Step	Command	Remarks
6. Specify an ACL to control SSH user connections.	- Control IPv4 SSH user connections: ssh server acl { <i>basic-acl-number</i> <i>advanced-acl-number</i> mac <i>mac-acl-number</i> } - Control IPv6 SSH user connections: ssh server ipv6 acl { ipv6 <i>basic-acl-number</i> ipv6 <i>advanced-acl-number</i> mac <i>mac-acl-number</i> }	By default, no ACLs are specified and all SSH users can initiate SSH connections to the server.
7. Set the DSCP value in the packets that the SSH server sends to the SSH clients.	- Set the DSCP value in IPv4 packets: ssh server dscp <i>dscp-value</i> - Set the DSCP value in IPv6 packets: ssh server ipv6 dscp <i>dscp-value</i>	The default setting is 48. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.
8. Set the SFTP connection idle timeout timer.	sftp server idle-timeout <i>time-out-value</i>	The default setting is 10 minutes. When the idle timeout timer expires, the system automatically tears the connection down.
9. Specify the maximum number of concurrent online SSH users.	aaa session-limit ssh <i>max-sessions</i>	The default setting is 32. When the number of online SSH users reaches the upper limit, the system denies new SSH connection requests. Changing the upper limit does not affect online SSH users.

Specifying a PKI domain for the SSH server

The PKI domain specified for the SSH server has the following functions:

- The SSH server uses the PKI domain to send its certificate to the client in the key exchange stage.
- The SSH server uses the PKI domain to authenticate the client's certificate if no PKI domain is specified for the client authentication by using the **ssh user** command.

To specify a PKI domain for the SSH server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a PKI domain for the SSH server.	ssh server pki-domain <i>domain-name</i>	By default, no PKI domain is specified for the SSH server.

Configuring the device as an Stelnet client

Stelnet client configuration task list

Tasks at a glance	Remarks
(Required.) Generating local DSA or RSA key pairs	Only required when the Stelnet server uses the authentication method publickey , password-publickey , or any .
(Optional.) Specifying the source IP address for SSH packets	N/A
(Required.) Establishing a connection to an Stelnet server	N/A
(Optional.) Establishing a connection to an Stelnet server based on Suite B	N/A

Generating local DSA or RSA key pairs

Generate local key pairs on the Stelnet client when the Stelnet server uses the authentication method **publickey**, **password-publickey**, or **any**.

Configuration restrictions and guidelines

When you generate local DSA or RSA key pairs on an Stelnet client, follow these restrictions and guidelines:

- The Stelnet client operating in FIPS mode supports only RSA key pairs. Do not generate local DSA key pairs when the device operates as an Stelnet client in FIPS mode.
- SSH supports locally generated DSA and RSA key pairs only with default names.
- The key modulus length must be less than 2048 bits when you generate a DSA key pair.

Configuration procedure

To generate local DSA or RSA key pairs on the Stelnet client:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Generate local DSA or RSA key pairs.	public-key local create { dsa rsa }	By default, no DSA or RSA key pairs exist on an Stelnet client.

Specifying the source IP address for SSH packets

As a best practice, specify the IP address of a loopback or dialer interface as the source address for SSH packets for the following purposes:

- Ensuring the communication between the Stelnet client and the Stelnet server.
- Improving the manageability of Stelnet clients in authentication service.

To specify the source IP address for SSH packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Specify the source address for SSH packets.	- Specify the source IPv4 address for SSH packets: ssh client source { interface interface-type interface-number ip ip-address } - Specify the source IPv6 address for SSH packets: ssh client ipv6 source { interface interface-type interface-number ipv6 ipv6-address }	By default, the source IP address for SSH packets is not configured. The IPv4 SSH packets use the primary IP address of the output interface specified in the routing entry as their source address. The IPv6 SSH packets automatically select an IPv6 address as their source address in compliance with RFC 3484.

Establishing a connection to an Stelnet server

When you try to access an Stelnet server, the device must use the server's host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server's host public key on the device in an insecure network.

The client cannot establish connections to both IPv4 and IPv6 Stelnet servers.

To establish a connection to an IPv4 Stelnet server:

Task	Command	Remarks
Establish a connection to an IPv4 Stelnet server.	- In non-FIPS mode: <code>ssh2 server [port-number] [vpn-instance vpn-instance-name] [identity-key { dsa rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } prefer-compress zlib prefer-ctos-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 }] * [dscp dscp-value escape character { public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ip ip-address }] *</code> - In FIPS mode: <code>ssh2 server [port-number] [vpn-instance vpn-instance-name] [identity-key rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name] prefer-compress zlib prefer-ctos-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { sha1 sha1-96 sha2-256 sha2-512 }] * [escape character { public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ip ip-address }] *</code>	Available in user view.

To establish a connection to an IPv6 Stelnet server:

Task	Command	Remarks
Establish a connection to an IPv6 Stelnet server.	- In non-FIPS mode: ssh2 ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [identity-key { dsa rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain <i>domain-name</i> } prefer-compress zlib prefer-ctos-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } } * [dscp <i>dscp-value</i> escape <i>character</i> { public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] * - In FIPS mode: ssh2 ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [identity-key rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain <i>domain-name</i> } prefer-compress zlib prefer-ctos-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { sha1 sha1-96 sha2-256 sha2-512 } } * [escape <i>character</i> { public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view.

Establishing a connection to an Stelnet server based on Suite B

Task	Command	Remarks
Establish a connection to an Stelnet server based on Suite B.	- Establish a connection to an IPv4 Stelnet server based on Suite B: <code>ssh2 server [port-number] [vpn-instance vpn-instance-name] suite-b [128-bit 192-bit] pki-domain domain-name [server-pki-domain domain-name] [prefer-compress zlib] [dscp dscp-value escape character source { interface interface-type interface-number ip ip-address }] *</code> - Establish a connection to an IPv6 Stelnet server based on Suite B: <code>ssh2 ipv6 server [port-number] [vpn-instance vpn-instance-name] suite-b [128-bit 192-bit] pki-domain domain-name [server-pki-domain domain-name] [interface interface-type interface-number] [prefer-compress zlib] [dscp dscp-value escape character source { interface interface-type interface-number ipv6 ipv6-address }] *</code>	Available in user view. The client cannot establish connections to both IPv4 and IPv6 Stelnet servers.

Configuring the device as an SFTP client

SFTP client configuration task list

Tasks at a glance	Remarks
(Required.) Generating local DSA or RSA key pairs	Only required when the SFTP server uses the authentication method publickey , password-publickey , or any .
(Optional.) Specifying the source IP address for SFTP packets	N/A
(Required.) Establishing a connection to an SFTP server	N/A
(Optional.) Establishing a connection to an SFTP server based on Suite B	N/A
(Optional.) Working with SFTP directories	N/A
(Optional.) Working with SFTP files	N/A
(Optional.) Displaying help information	N/A
(Optional.) Terminating the connection with the SFTP server	N/A

Generating local DSA or RSA key pairs

Generate local key pairs on the SFTP client when the SFTP server uses the authentication method **publickey**, **password-publickey**, or **any**.

Configuration restrictions and guidelines

When you generate local DSA or RSA key pairs on an SFTP client, follow these restrictions and guidelines:

- SSH supports locally generated DSA and RSA key pairs only with default names.
- The SFTP client operating in FIPS mode supports only RSA key pairs. Do not generate local DSA key pairs when the device operates as an SFTP client in FIPS mode.
- The key modulus length must be less than 2048 bits when you generate a DSA key pair.

Configuration procedure

To generate local DSA or RSA key pairs on the SFTP client:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Generate local DSA or RSA key pairs.	public-key local create { dsa rsa }	By default, no DSA or RSA key pairs exist on an SFTP client.

Specifying the source IP address for SFTP packets

As a best practice, specify the IP address of a loopback or dialer interface as the source address for SFTP packets for the following purposes:

- Ensuring the communication between the SFTP client and the SFTP server.
- Improving the manageability of SFTP clients in authentication service.

To specify the source IP address for SFTP packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the source address for SFTP packets.	• Specify the source IPv4 address for SFTP packets: sftp client source { ip ip-address interface interface-type interface-number } • Specify the source IPv6 address for SFTP packets: sftp client ipv6 source { ipv6 ipv6-address interface interface-type interface-number }	By default, the source IP address for SFTP packets is not configured. The IPv4 SFTP packets use the primary IP address of the output interface specified in the routing entry as their source IP address. The IPv6 SFTP packets automatically select an IPv6 address as their source address in compliance with RFC 3484.

Establishing a connection to an SFTP server

When you try to access an SFTP server, the device must use the server's host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server's host public key on the device in an insecure network.

After the connection is established, you can directly enter SFTP client view on the server to perform file or directory operations.

The client cannot establish connections to both IPv4 and IPv6 SFTP servers.

To establish a connection to an IPv4 SFTP server:

Task	Command	Remarks
Establish a connection to an IPv4 SFTP server.	- In non-FIPS mode: sftp server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [identity-key { <i>dsa</i> <i>rsa</i> { <i>x509v3-ecdsa-sha2-nistp384</i> <i>x509v3-ecdsa-sha2-nistp256</i> } pki-domain <i>domain-name</i> } prefer-compress <i>zlib</i> prefer-ctos-cipher { <i>3des-cbc</i> <i>aes128-cbc</i> <i>aes256-cbc</i> <i>des-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-ctos-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } prefer-kex { <i>dh-group-exchange-sha1</i> <i>dh-group1-sha1</i> <i>dh-group14-sha1</i> <i>ecdh-sha2-nistp256</i> <i>ecdh-sha2-nistp384</i> } prefer-stoc-cipher { <i>3des-cbc</i> <i>aes128-cbc</i> <i>aes256-cbc</i> <i>des-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-stoc-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } } * [dscp <i>dscp-value</i> { public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type interface-number</i> ip <i>ip-address</i> }] * - In FIPS mode: sftp server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [identity-key <i>rsa</i> { <i>x509v3-ecdsa-sha2-nistp384</i> <i>x509v3-ecdsa-sha2-nistp256</i> } pki-domain <i>domain-name</i> } prefer-compress <i>zlib</i> prefer-ctos-cipher { <i>aes128-cbc</i> <i>aes256-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-ctos-hmac { <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } prefer-kex { <i>dh-group14-sha1</i> <i>ecdh-sha2-nistp256</i> <i>ecdh-sha2-nistp384</i> } prefer-stoc-cipher { <i>aes128-cbc</i> <i>aes256-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-stoc-hmac { <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } } * [{ public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type interface-number</i> ip <i>ip-address</i> }] *	Available in user view.

To establish a connection to an IPv6 SFTP server:

Task	Command	Remarks
Establish a connection to an IPv6 SFTP server.	- In non-FIPS mode: sftp ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [identity-key { <i>dsa</i> <i>rsa</i> { <i>x509v3-ecdsa-sha2-nistp384</i> <i>x509v3-ecdsa-sha2-nistp256</i> } pki-domain <i>domain-name</i> } prefer-compress <i>zlib</i> prefer-ctos-cipher { <i>3des-cbc</i> <i>aes128-cbc</i> <i>aes256-cbc</i> <i>des-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-ctos-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } prefer-kex { <i>dh-group-exchange-sha1</i> <i>dh-group1-sha1</i> <i>dh-group14-sha1</i> <i>ecdh-sha2-nistp256</i> <i>ecdh-sha2-nistp384</i> } prefer-stoc-cipher { <i>3des-cbc</i> <i>aes128-cbc</i> <i>aes256-cbc</i> <i>des-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-stoc-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } } * [dscp <i>dscp-value</i> { public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] * - In FIPS mode: sftp ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [identity-key <i>rsa</i> { <i>x509v3-ecdsa-sha2-nistp384</i> <i>x509v3-ecdsa-sha2-nistp256</i> } pki-domain <i>domain-name</i> } prefer-compress <i>zlib</i> prefer-ctos-cipher { <i>aes128-cbc</i> <i>aes256-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-ctos-hmac { <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } prefer-kex { <i>dh-group14-sha1</i> <i>ecdh-sha2-nistp256</i> <i>ecdh-sha2-nistp384</i> } prefer-stoc-cipher { <i>aes128-cbc</i> <i>aes256-cbc</i> <i>aes128-ctr</i> <i>aes192-ctr</i> <i>aes256-ctr</i> <i>aes128-gcm</i> <i>aes256-gcm</i> } prefer-stoc-hmac { <i>sha1</i> <i>sha1-96</i> <i>sha2-256</i> <i>sha2-512</i> } } * [{ public-key <i>keyname</i> server-pki-domain <i>domain-name</i> } source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view.

Establishing a connection to an SFTP server based on Suite B

After the connection is established, you are in SFTP client view of the server and can perform file or directory operations.

To establish a connection to an SFTP server based on Suite B:

Task	Command	Remarks
Establish a connection to an SFTP server based on Suite B.	- Establish a connection to an IPv4 SFTP server based on Suite B: sftp server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> }] * - Establish a connection to an IPv6 SFTP server based on Suite B: sftp ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [interface <i>interface-type</i> <i>interface-number</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SFTP servers.

Working with SFTP directories

Task	Command	Remarks
Change the working directory on the SFTP server.	cd [<i>remote-path</i>]	Available in SFTP client view.
Return to the upper-level directory.	cdup	Available in SFTP client view.
Display the current working directory on the SFTP server.	pwd	Available in SFTP client view.
Display files under a directory.	dir [-a -l] [<i>remote-path</i>] ls [-a -l] [<i>remote-path</i>]	Available in SFTP client view. The dir command has the same function as the ls command.
Change the name of a directory on the SFTP server.	rename <i>oldname newname</i>	Available in SFTP client view.
Create a new directory on the SFTP server.	mkdir <i>remote-path</i>	Available in SFTP client view.
Delete one or more directories from the SFTP server.	rmdir <i>remote-path</i>	Available in SFTP client view.

Working with SFTP files

Task	Command	Remarks
Change the name of a file on the SFTP server.	rename <i>old-name new-name</i>	Available in SFTP client view.
Download a file from the SFTP server and save it locally.	get <i>remote-file</i> [<i>local-file</i>]	Available in SFTP client view.
Upload a local file to the SFTP server.	put <i>local-file</i> [<i>remote-file</i>]	Available in SFTP client view.

Task	Command	Remarks
Display files under a directory.	dir [-a -l] [<i>remote-path</i>] ls [-a -l] [<i>remote-path</i>]	Available in SFTP client view. The dir command has the same function as the ls command.
Delete one or more directories from the SFTP server.	delete <i>remote-file</i> remove <i>remote-file</i>	Available in SFTP client view. The delete command has the same function as the remove command.

Displaying help information

Task	Command	Remarks
Display the help information of SFTP client commands.	help ?	Available in SFTP client view.

Terminating the connection with the SFTP server

Task	Command	Remarks
Terminate the connection with the SFTP server and return to user view.	bye exit quit	Available in SFTP client view. These three commands have the same function.

Configuring the device as an SCP client

SCP client configuration task list

Tasks at a glance	Remarks
(Required.) Generating local DSA or RSA key pairs	Only required when the SCP server uses the authentication method publickey , password-publickey , or any .
(Required.) Establishing a connection to an SCP server	N/A
(Optional.) Establishing a connection to an SCP server based on Suite B	N/A

Generating local DSA or RSA key pairs

Generate local key pairs on the SCP client when the SCP server uses the authentication method **publickey**, **password-publickey**, or **any**.

Configuration restrictions and guidelines

When you generate local DSA or RSA key pairs on an SCP client, follow these restrictions and guidelines:

- SSH supports locally generated DSA and RSA key pairs only with default names.

- The SCP client operating in FIPS mode supports only RSA key pairs. Do not generate local DSA key pairs when the device operates as an SCP client in FIPS mode.
- The key modulus length must be less than 2048 bits when you generate a DSA key pair.

Configuration procedure

To generate local DSA or RSA key pairs on the SCP client:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Generate local DSA or RSA key pairs.	public-key local create { dsa rsa }	By default, no DSA or RSA key pairs exist on an SCP client.

Establishing a connection to an SCP server

When you try to access an SCP server, the device must use the server's host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server's host public key on the device in an insecure network.

The client cannot establish connections to both IPv4 and IPv6 SCP servers.

To establish a connection to an IPv4 SCP server:

Task	Command	Remarks
Connect to an IPv4 SCP server, and transfer files with the server.	- In non-FIPS mode: <code>scp server [port-number] [vpn-instance vpn-instance-name] { put get } source-file-name [destination-file-name] [identity-key { dsa rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } prefer-compress zlib prefer-ctos-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } } *</code> <code>[{ public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ip ip-address }] *</code> - In FIPS mode: <code>scp server [port-number] [vpn-instance vpn-instance-name] { put get } source-file-name [destination-file-name] [identity-key rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } prefer-compress zlib prefer-ctos-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { sha1 sha1-96 sha2-256 sha2-512 } } * [{ public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ip ip-address }] *</code>	Available in user view.

To establish a connection to an IPv6 SCP server:

Task	Command	Remarks
Connect to an IPv6 SCP server, and transfer files with the server.	- In non-FIPS mode: scp ipv6 server [port-number] [vpn-instance vpn-instance-name] [-i interface-type interface-number] { put get } source-file-name [destination-file-name] [identity-key { dsa rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } prefer-compress zlib prefer-ctos-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } } * [{ public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ipv6 ipv6-address }] * - In FIPS mode: scp ipv6 server [port-number] [vpn-instance vpn-instance-name] [-i interface-type interface-number] { put get } source-file-name [destination-file-name] [identity-key rsa { x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } prefer-compress zlib prefer-ctos-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-ctos-hmac { sha1 sha1-96 sha2-256 sha2-512 } prefer-kex { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } prefer-stoc-cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } prefer-stoc-hmac { sha1 sha1-96 sha2-256 sha2-512 } } * [{ public-key keyname server-pki-domain domain-name } source { interface interface-type interface-number ipv6 ipv6-address }] *	Available in user view.

Establishing a connection to an SCP server based on Suite B

Task	Command	Remarks
Establish a connection to an SCP server based on Suite B.	- Establish a connection to an IPv4 SCP server based on Suite B: scp server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] { put get } <i>source-file-name</i> [<i>destination-file-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [prefer-compress zlib] [source { interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> }] * - Establish a connection to an IPv6 SCP server based on Suite B: scp ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] [interface <i>interface-type</i> <i>interface-number</i>] { put get } <i>source-file-name</i> [<i>destination-file-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [prefer-compress zlib] [source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SCP servers.

Specifying algorithms for SSH2

Perform this task to specify the following types of algorithms that the SSH2 client and server use for algorithm negotiation during the Stelnet, SFTP, or SCP session establishment:

- Key exchange algorithms.
- Public key algorithms.
- Encryption algorithms.
- MAC algorithms.

If you specify algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The client uses the specified algorithms to initiate the negotiation, and the server uses the matching algorithms to negotiate with the client.

If multiple algorithms of the same type are specified, the algorithm specified earlier has a higher priority during negotiation. The specified SSH2 algorithms do not affect SSH1 sessions.

Specifying key exchange algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify key exchange algorithms for SSH2.	In non-FIPS mode: ssh2 algorithm key-exchange { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } *	By default, SSH2 uses the key exchange algorithms ecdh-sha2-nistp256 , ecdh-sha2-nistp384 , dh-group-exchange-sha1 , dh-group14-sha1 , and dh-group1-sha1 in descending order of priority for algorithm

Step	Command	Remarks
	In FIPS mode: ssh2 algorithm key-exchange { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } *	negotiation.

Specifying public key algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify public key algorithms for SSH2.	- In non-FIPS mode: ssh2 algorithm public-key { dsa rsa x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } * - In FIPS mode: ssh2 algorithm public-key { rsa x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } *	By default, SSH2 uses the public key algorithms x509v3-ecdsa-sha2-nistp256 , x509v3-ecdsa-sha2-nistp384 , rsa , and dsa in descending order of priority for algorithm negotiation.

Specifying encryption algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify encryption algorithms for SSH2.	- In non-FIPS mode: ssh2 algorithm cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } * - In FIPS mode: ssh2 algorithm cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } *	By default, SSH2 uses the encryption algorithms aes128-ctr , aes192-ctr , aes256-ctr , aes128-gcm , aes256-gcm , aes128-cbc , 3des-cbc , aes256-cbc , and des-cbc in descending order of priority for algorithm negotiation.

Specifying MAC algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify MAC algorithms for SSH2.	In non-FIPS mode: ssh2 algorithm mac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } *	By default, SSH2 uses the MAC algorithms sha2-256 , sha2-512 , sha1 , md5 , sha1-96 , and md5-96 in descending order of priority for

Step	Command	Remarks
	In FIPS mode: <code>ssh2 algorithm mac { sha1 sha1-96 sha2-256 sha2-512 } *</code>	algorithm negotiation.

Displaying and maintaining SSH

Execute **display** commands in any view.

Task	Command
Display the source IP address configured for the SFTP client.	display sftp client source
Display the source IP address configured for the Stelnet client.	display ssh client source
Display SSH server status or sessions.	display ssh server { session status }
Display SSH user information on the SSH server.	display ssh user-information [username]
Display the public keys of the local key pairs.	display public-key local { dsa rsa } public [name <i>publickey-name</i>]
Display information about peer public keys.	display public-key peer [brief name <i>publickey-name</i>]
Display algorithms used by SSH2 in the algorithm negotiation stage.	display ssh2 algorithm

Stelnet configuration examples

Unless otherwise noted, devices in the configuration examples operate in non-FIPS mode.

When you configure Stelnet on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as an Stelnet server, only RSA key pairs are supported. Do not generate a DSA key pair on the Stelnet server.

Password authentication enabled Stelnet server configuration example

Network requirements

As shown in [Figure 116](#):

- The router acts as the Stelnet server and uses password authentication.
- The username and password of the client are saved on the router.

Establish a connection between the host and the router, so you can log in to the router to manage configurations.

The diagram illustrates a network connection between a Stelnet client and a Stelnet server. On the left, a blue computer icon represents the 'Host' (Stelnet client) with the IP address 192.168.1.56/24. On the right, a blue router icon represents the 'Router' (Stelnet server) with the IP address 192.168.1.40/24. A black line connects the two, with the interface 'GE2/0/1' labeled above it. The router icon also has the word 'ROUTER' written below it.

1. Configure the Stelnet server:

```
<Router> system-view
```

The range of public key size is (512 ~ 2048).

Press CTRL+C to abort.

Generating Keys...

.....+++++

. . ++++++

. ++++++

```
# Generate a DSA key pair.
```

The range of public key size is (512 ~ 2048).

Press CTRL+C to abort.

Generating Keys...

,+++++*****

.....+.....+.....+.....+

.....+.....+.....+.....+

```
# Enable the Stelnet server.
```

Assign an IP address to GigabitEthernet 2/0/1. The Stelnet client uses this IP address as the destination for SSH connection.

```
[Router-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
```

```
[Router-GigabitEthernet2/0/1] quit
```

```
# Set the authentication mode to AAA for the user lines.
```

```
[Router-line-vty0-15] authentication-mode scheme
```

```
[Router-line-vty0-15] quit
```

```
# Create a local device management user named client001.
```

```
[Router] local-user client001 class manage
```

```
# Set the password to aabbcc in plain text for the local user client001.
```

```
[Router-luser-manage-client001] password simple aabbcc
```

Authorize the local user **client001** to use the **SSH** service.

```
[Router-luser-manage-client001] service-type ssh
```

Assign the **network-admin** user role to the local user **client001**.

```
[Router-luser-manage-client001] authorization-attribute user-role network-admin
```

```
[Router-luser-manage-client001] quit
```

Create an SSH user named **client001**. Specify the service type as **stelnet** and the authentication method as **password** for the user.

```
[Router] ssh user client001 service-type stelnet authentication-type password
```

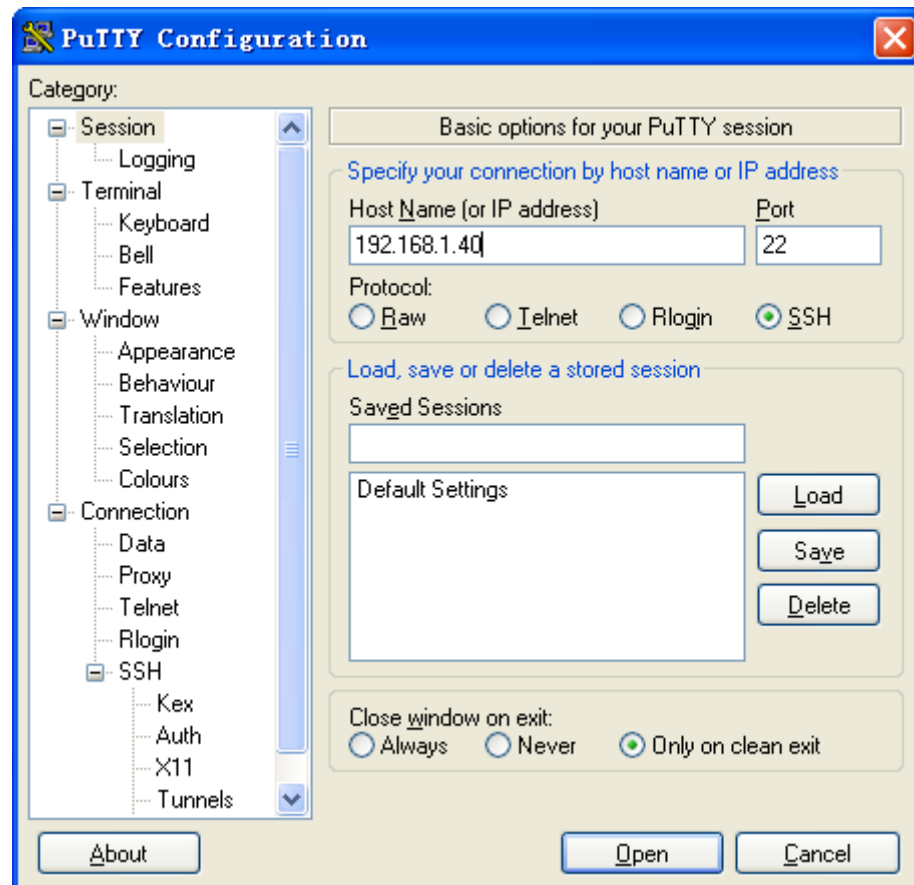
2. Establish a connection to the Stelnet server:

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

To establish a connection to the Stelnet server:

- a. Launch PuTTY.exe to enter the interface shown in [Figure 117](#).
- b. In the **Host Name (or IP address)** field, enter the IP address **192.168.1.40** of the Stelnet server.

Figure 117 Specifying the host name (or IP address)



- c. Click **Open** to connect to the server.

If the connection is successfully established, the system notifies you to enter the username and password. After entering the username (**client001**) and password (**aabbcc**), you can enter the CLI of the server.

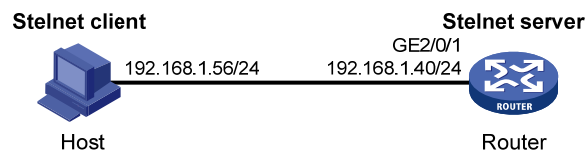
Publickey authentication enabled Stelnet server configuration example

Network requirements

As shown in [Figure 118](#), the router acts as the Stelnet server, and it uses publickey authentication and the RSA public key algorithm.

Establish a connection between the host and the router, so you can log in to the router to manage configurations.

Figure 118 Network diagram



Configuration procedure

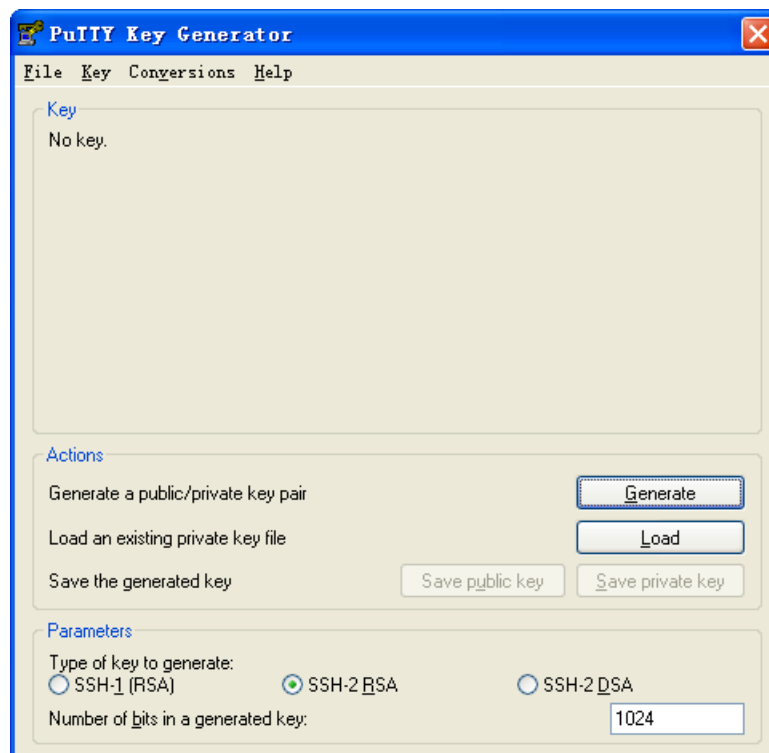
In the server configuration, the client's host public key is required. Use the client software to generate RSA key pairs on the client before configuring the Stelnet server.

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

The configuration procedure is as follows:

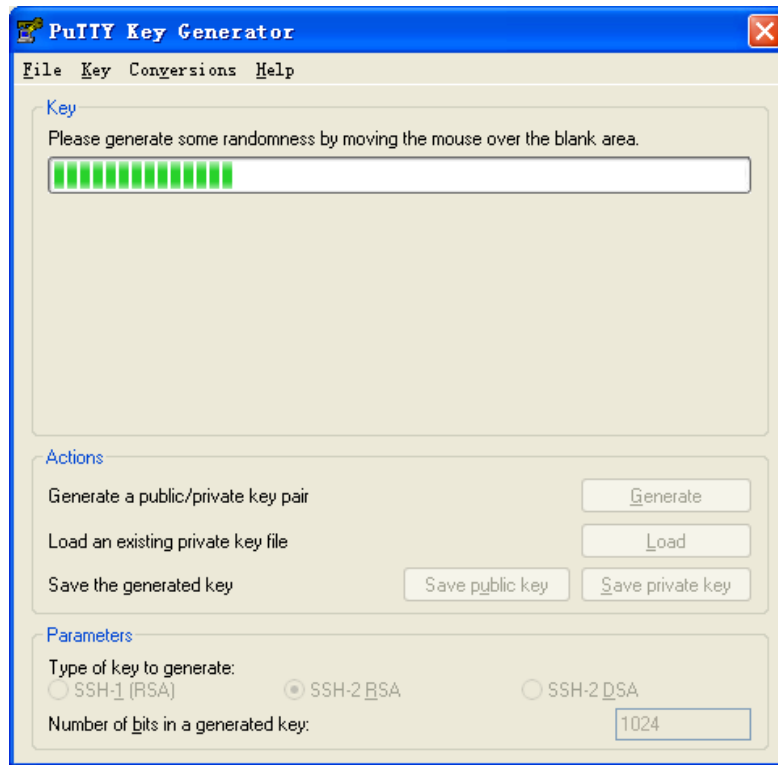
1. Generate RSA key pairs on the Stelnet client:
 - a. Run PuTTYGen.exe, select **SSH-2 RSA** and click **Generate**.

Figure 119 Generating a key pair on the client



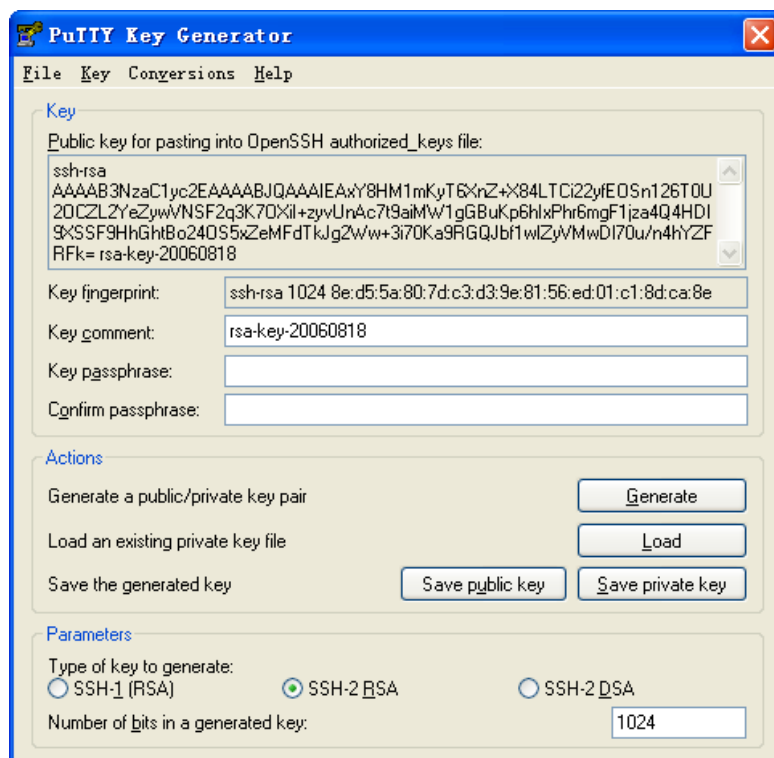
- b. Continuously move the mouse and do not place the mouse over the green progress bar shown in Figure 120. Otherwise, the progress bar stops moving and the key pair generating process stops.

Figure 120 Generating process



- c. After the key pair is generated, click **Save public key** to save the public key. A file saving window appears.

Figure 121 Saving a key pair on the client



- d. Enter a file name (**key.pub** in this example), and click **Save**.
 - e. On the page as shown in Figure 121, click **Save private key** to save the private key.
A confirmation dialog box appears.
 - f. Click **Yes**.
A file saving window appears.
 - g. Enter a file name (**private.ppk** in this example), and click **Save**.
 - h. Transmit the public key file to the server through FTP or TFTP. (Details not shown.)
2. Configure the Stelnet server:

Generate RSA key pairs.

```
<Router> system-view
```

```
[Router] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....++++++

.....++++++

..++++++

.....++++++

Create the key pair successfully.

Generate a DSA key pair.

```
[Router] public-key local create dsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

```
.+++++*
.....+.....+.....+.....+
...+.....+.....+.....+
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Router] ssh server enable
```

Assign an IP address to GigabitEthernet 2/0/1. The Stelnet client uses this address as the destination for SSH connection.

```
[Router] interface gigabitethernet 2/0/1
```

```
[Router-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
```

```
[Router-GigabitEthernet2/0/1] quit
```

Set the authentication mode to AAA for the user lines.

```
[Router] line vty 0 15
```

```
[Router-line-vty0-15] authentication-mode scheme
```

```
[Router-line-vty0-15] quit
```

Import the peer public key from file **key.pub** and name it **clientkey**.

```
[Router] public-key peer clientkey import sshkey key.pub
```

Create an SSH user named **client002**. Specify the authentication method as **publickey** for the user, and assign the public key **clientkey** to the user.

```
[Router] ssh user client002 service-type stelnet authentication-type publickey assign publickey clientkey
```

Create a local device management user named **client002**.

```
[Router] local-user client002 class manage
```

Authorize the local user **client002** to use the **SSH** service.

```
[Router-luser-manage-client002] service-type ssh
```

Assign the **network-admin** user role to the user **client002**.

```
[Router-luser-manage-client002] authorization-attribute user-role network-admin
```

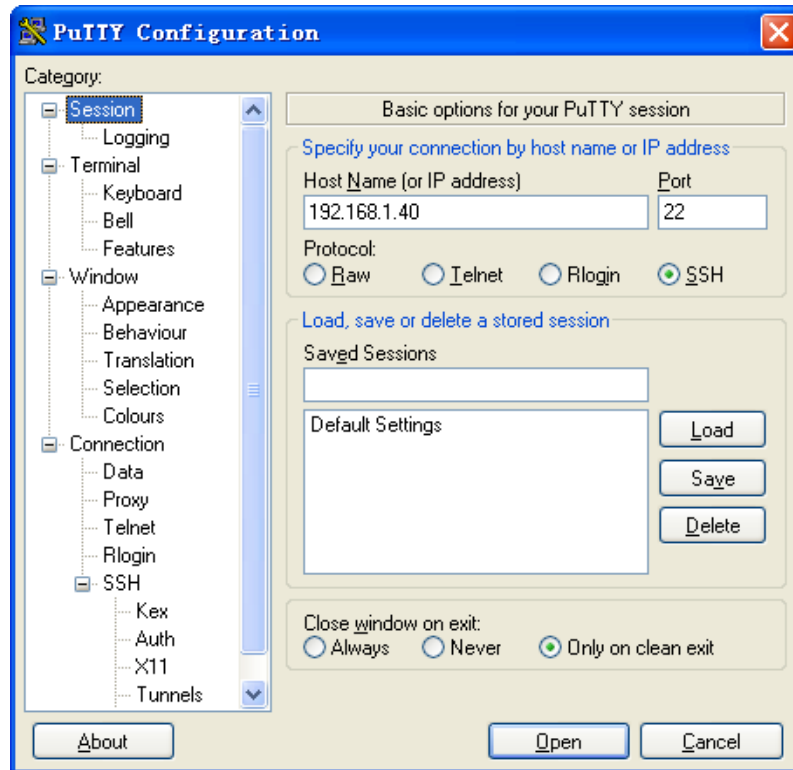
```
[Router-luser-manage-client002] quit
```

3. Specify the private key file and establish a connection to the Stelnet server:

a. Launch PuTTY.exe on the Stelnet client to enter the interface shown in [Figure 122](#).

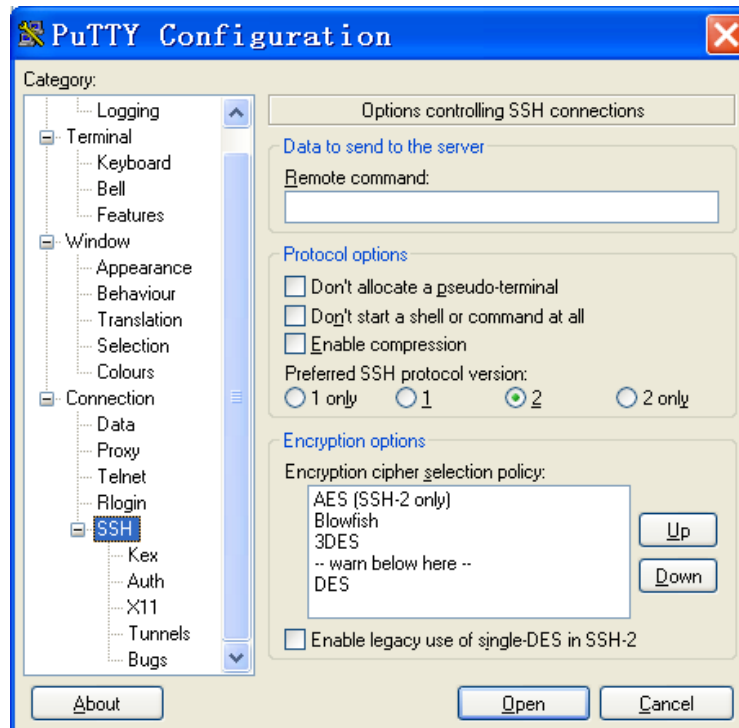
b. In the **Host Name (or IP address)** field, enter the IP address **192.168.1.40** of the Stelnet server.

Figure 122 Specifying the host name (or IP address)



- c. Select **Connection** > **SSH** from the navigation tree.
The window shown in Figure 123 appears.
- d. Specify the **Preferred SSH protocol version** as 2.

Figure 123 Specifying the preferred SSH version

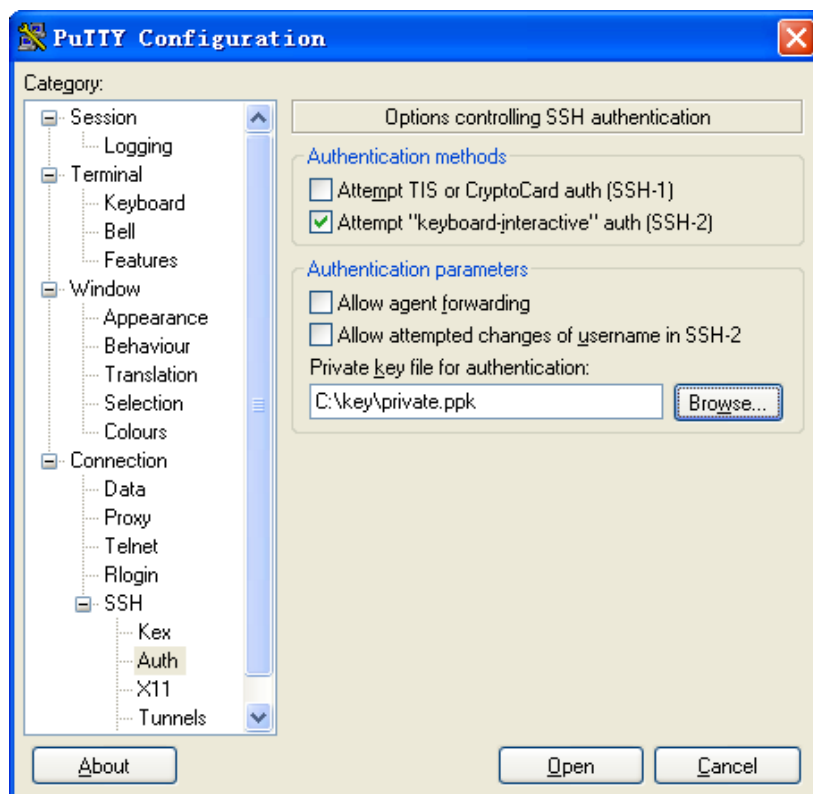


- e. Select **Connection** > **SSH** > **Auth** from the navigation tree.

The window shown in Figure 124 appears.

- f. Click **Browse...** to bring up the file selection window, navigate to the private key file (**private.ppk** in this example), and click **OK**.

Figure 124 Specifying the private key file



- g. Click **Open** to connect to the server.

If the connection is successfully established, the system notifies you to enter the username. After entering the username (**client002**), you can enter the CLI of the server.

Password authentication enabled Stelnet client configuration example

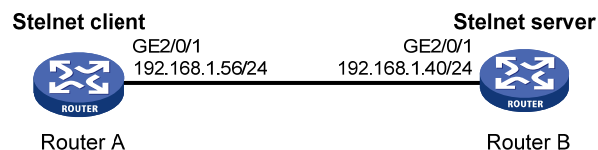
Network requirements

As shown in Figure 125:

- Router B acts as the Stelnet server and uses password authentication.
- The username and password of the client are saved on Router B.

Establish a connection between Router A and Router B, so you can log in to Router B to manage configurations.

Figure 125 Network diagram



Configuration procedure

- ## 1. Configure the Stelnet server:

```
# Generate RSA key pairs.
```

```
<RouterB> system-view
```

```
[RouterB] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....+++++

.....+++++

. . ++++++

. ++++++

Create the key pair successfully.

```
# Generate a DSA key pair.
```

```
[RouterB] public-key local create dsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

,+++++*****

.....+.....+.....+.....+

.....+.....+.....+.....+

Create the key pair successfully.

```
# Enable the Stelnet server.
```

```
[RouterB] ssh server enable
```

Assign an IP address to GigabitEthernet 2/0/1. The Stelnet client uses this address as the destination address for SSH connection.

```
[RouterB] interface gigabitethernet 2/0/1
```

```
[RouterB-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
```

```
[RouterB-GigabitEthernet2/0/1] quit
```

```
# Set the authentication mode to AAA for the user lines.
```

```
[RouterB] line vty 0 15
```

```
[RouterB-line-vty0-15] authentication-mode scheme
```

```
[RouterB-line-vty0-15] quit
```

```
# Create a local device management user named client001.
```

```
[RouterB] local-user client001 class manage
```

```
# Set the password to aabbcc in plain text for the local user client001.
```

```
[RouterB-luser-manage-client001] password simple aabbcc
```

```
# Authorize the local user client001 to use the SSH service.
```

```
[RouterB-luser-manage-client001] service-type ssh
```

```
# Assign the network-admin user role to the local user client001.
```

```
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
```

```
[RouterB-luser-manage-client001] quit
```

Create an SSH user named **client001**. Specify the service type as **stelnet** and the authentication method as **password** for the user.

```
[RouterB] ssh user client001 service-type stelnet authentication-type password
```

2. Establish a connection to the Stelnet server 192.168.1.40:

Assign an IP address to GigabitEthernet 2/0/1.

```
<RouterA> system-views
```

```
[RouterA] interface gigabitethernet 2/0/1
```

```
[RouterA-GigabitEthernet2/0/1] ip address 192.168.1.56 255.255.255.0
```

```
[RouterA-GigabitEthernet2/0/1] quit
```

```
[RouterA] quit
```

Before establishing a connection to the server, you can configure the server's host public key on the client to authenticate the server.

- o To configure the server's host public key on the client, perform the following tasks:

Use the **display public-key local rsa public** command on the server to display the server's host public key. (Details not shown.)

Enter public key view of the client and copy the host public key of the server to the client.

```
[RouterA] public-key peer key1
```

Enter public key view. Return to system view with "peer-public-key end" command.

```
[RouterA-pkey-public-key-key1]
```

```
308201B73082012C06072A8648CE3804013082011F0281810
```

```
0D757262C4584C44C211F18BD96E5F0
```

```
[RouterA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CEC  
E
```

```
65BE6C265854889DC1EDBD13EC8B274
```

```
[RouterA-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B  
0
```

```
6FD60FE01941DDD77FE6B12893DA76E
```

```
[RouterA-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B  
3
```

```
68950387811C7DA33021500C773218C
```

```
[RouterA-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082269009  
E
```

```
14EC474BAF2932E69D3B1F18517AD95
```

```
[RouterA-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D0  
2
```

```
492B3959EC6499625BC4FA5082E22C5
```

```
[RouterA-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2  
E
```

```
88317C1BD8171D41ECB83E210C03CC9
```

```
[RouterA-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718C  
C
```

```
9B09EEF0381840002818000AF995917
```

```
[RouterA-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5  
D
```

```
F257523777D033BEE77FC378145F2AD
```

```
[RouterA-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F7  
1
```

```
01F7C62621216D5A572C379A32AC290
```

```
[RouterA-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465  
E
```

```

8716261214A5A3B493E866991113B2D
[RouterA-pkey-public-key-key1]485348
[RouterA-pkey-public-key-key1] peer-public-key end
[RouterA] quit
# Establish an SSH connection to the server, and specify the host public key of the server as
key1.
<RouterA> ssh2 192.168.1.40 publickey key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

```

```

*****
* Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

```

<RouterB>

After you enter the correct password, you log in to Router B successfully.

- If the client does not have the server's host public key, the system will notify you to confirm the further access when you access the server. Select **Yes** to access the server and download the server's host public key.

```

<RouterA> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

```

```

*****
* Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

```

<RouterB>

After you enter the correct password, you can access Router B successfully. At the next connection attempt, the client authenticates the server by using the saved server's host public key on the client.

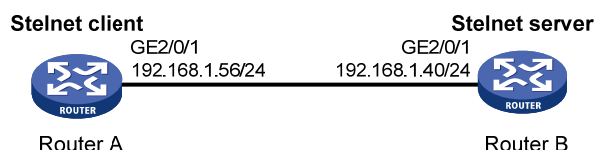
Publickey authentication enabled Stelnet client configuration example

Network requirements

As shown in [Figure 126](#), Router B acts as the Stelnet server, and it uses publickey authentication and the DSA public key algorithm.

Establish an Stelnet connection between Router A and Router B, so you can log in to Router B to manage configurations.

Figure 126 Network diagram



Configuration procedure

In the server configuration, the client's host public key is required. Generate a DSA key pair on the client before configuring the Stelnet server.

1. Configure the Stelnet client:

Assign an IP address to GigabitEthernet 2/0/1.

```
<RouterA> system-view
```

```
[RouterA] interface gigabitethernet 2/0/1
```

```
[RouterA-GigabitEthernet2/0/1] ip address 192.168.1.56 255.255.255.0
```

```
[RouterA-GigabitEthernet2/0/1] quit
```

Generate a DSA key pair.

```
[RouterA] public-key local create dsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.+*****+

.....+......+......+......+

...+......+......+......+

Create the key pair successfully.

Export the DSA host public key to the file **key.pub**.

```
[RouterA] public-key local export dsa ssh2 key.pub
```

```
[RouterA] quit
```

Transmit the public key file **key.pub** to the server through FTP or TFTP. (Details not shown.)

2. Configure the Stelnet server:

Generate RSA key pairs.

```
<RouterB> system-view
```

```
[RouterB] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

```

.....++++++
.....++++++
..+++++++
.....+++++++

```

```
# Generate a DSA key pair.
```

The range of public key size is (512 ~ 2048).

Press CTRL+C to abort.

Generating Keys...

```
.+++++*****  
.....+. ....+. ....+. .....+  
.+. ....+. ....+. ....+
```

```
# Enable the Stelnet server.
```

Assign an IP address to GigabitEthernet 2/0/1. The Stelnet client uses this address as the destination address for SSH connection.

```
[RouterB-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
```

```
[RouterB-GigabitEthernet2/0/1] quit
```

```
# Set the authentication mode to AAA for the user lines.
```

```
[RouterB-line-vty0-15] authentication-mode scheme
```

```
[RouterB-line-vty0-15] quit
```

```
# Import the peer public key from the file key.pub, and name it clientkey.
```

```
[RouterB] public-key peer clientkey import sshkey key.pub
```

Create an SSH user named **client002**. Specify the authentication method as **publickey** for the user, and assign the public key **clientkey** to the user.

```
[RouterB] ssh user client002 service-type stelnet authentication-type publickey
assign publickey clientkey
```

```
# Create a local device management user named client002.
```

```
[RouterB] local-user client002 class manage
```

```
# Authorize the local user client002 to use the SSH service.
```

```
[RouterB-luser-manage-client002] service-type ssh
```

```
# Assign the network-admin user role to the local user client002.
```

```
[RouterB-luser-manage-client002] authorization-attribute user-role network-admin
```

```
[RouterB-luser-manage-client002] quit
```

```
<RouterA> ssh2 192.168.1.40
```

```
Username: client002
```

Press CTRL+C to abort.

```
Connecting to 192.168.1.40 port 22.
```

```
The server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

Enter a character ~ and a dot to abort.

```
*****
* Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
*****
```

<RouterB>

Select **Yes** to access the server and download the server's host public key. At the next connection attempt, the client authenticates the server by using the saved server's host public key on the client.

Stelnet configuration example based on 128-bit Suite B algorithms

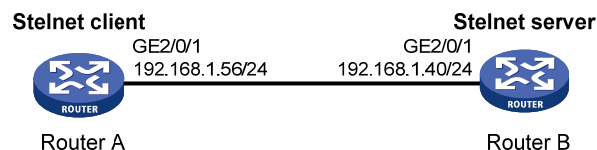
Network requirements

As shown in [Figure 127](#):

- Router A acts as an Stelnet client (SSH2).
- Router B acts as the Stelnet server (SSH2), and it uses publickey authentication.
- Router B uses the following algorithms for the algorithm negotiation with the Stelnet client:
 - Key exchange algorithm **ecdh-sha2-nistp256**.
 - Encryption algorithm **aes128-gcm**.
 - Public key algorithms **x509v3-ecdsa-sha2-nistp256** and **x509v3-ecdsa-sha2-nistp384**.

Configure Router A to establish an Stelnet connection to Router B based on the 128-bit Suite B algorithms. After the connection is established, you can log in to Router B to configure and manage Router B.

Figure 127 Network diagram



Configuration procedure

1. Generate the client's certificate and the server's certificate. (Details not shown.)
You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.
In this example, the server's certificate file is **ssh-server-ecdsa256.p12** and the client's certificate file is **ssh-client-ecdsa256.p12**.
2. Configure the Stelnet client:

NOTE:

You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE router as an Stelnet client.

Upload the server's certificate file **ssh-server-ecdsa256.p12** and the client's certificate file **ssh-client-ecdsa256.p12** to the Stelnet client through FTP or TFTP. (Details not shown.)

```

# Create a PKI domain named server256 for verifying the server's certificate and enter its view.
<RouterA> system-view
[RouterA] pki domain server256
# Disable CRL checking.
[RouterA-pki-domain-server256] undo crl check enable
[RouterA-pki-domain-server256] quit
# Import the local certificate file ssh-server-ecdsa256.p12 to the PKI domain server256.
[RouterA] pki import domain server256 p12 local filename ssh-server-ecdsa256.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: server256]:
# Display information about local certificates in the PKI domain server256.
[RouterA] display pki certificate domain server256 local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
    Validity
        Not Before: Aug 21 08:39:51 2015 GMT
        Not After : Aug 20 08:39:51 2016 GMT
        Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=SSH Server secp256
    Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        pub:
            04:a2:b4:b4:66:1e:3b:d5:50:50:0e:55:19:8d:52:
            6d:47:8c:3d:3d:96:75:88:2f:9a:ba:a2:a7:f9:ef:
            0a:a9:20:b7:b6:6a:90:0e:f8:c6:de:15:a2:23:81:
            3c:9e:a2:b7:83:87:b9:ad:28:c8:2a:5e:58:11:8e:
            c7:61:4a:52:51
        ASN1 OID: prime256v1
        NIST CURVE: P-256
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            08:C1:F1:AA:97:45:19:6A:DA:4A:F2:87:A1:1A:E8:30:BD:31:30:D7
        X509v3 Authority Key Identifier:
            keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

    Signature Algorithm: ecdsa-with-SHA256
        30:65:02:31:00:a9:16:e9:c1:76:f0:32:fc:4b:f9:8f:b6:7f:
        31:a0:9f:de:a7:cc:33:29:27:2c:71:2e:f9:0d:74:cb:25:c9:

```

```
00:d2:52:18:7f:58:3f:cc:7e:8b:d3:42:65:00:cb:63:f8:02:
30:01:a2:f6:a1:51:04:1c:61:78:f6:6b:7e:f9:f9:42:8d:7c:
a7:bb:47:7c:2a:85:67:0d:81:12:0b:02:98:bc:06:1f:c1:3c:
9b:c2:1b:4c:44:38:5a:14:b2:48:63:02:2b
```

Create a PKI domain named **client256** for the client's certificate and enter its view.

```
[RouterA] pki domain client256
```

Disable CRL checking.

```
[RouterA-pki-domain-client256] undo crl check enable
```

```
[RouterA-pki-domain-client256] quit
```

Import the local certificate file **ssh-client-ecdsa256.p12** to the PKI domain **client256**.

```
[RouterA] pki import domain client256 p12 local filename ssh-client-ecdsa256.p12
```

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name[default name: client256]:

Display information about local certificates in the PKI domain **client256**.

```
[RouterA] display pki certificate domain client256 local
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 4 (0x4)

Signature Algorithm: ecdsa-with-SHA256

Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA

Validity

Not Before: Aug 21 08:41:09 2015 GMT

Not After : Aug 20 08:41:09 2016 GMT

Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=SSH Client secp256

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:da:e2:26:45:87:7a:63:20:e7:ca:7f:82:19:f5:

96:88:3e:25:46:f8:2f:9a:4c:70:61:35:db:e4:39:

b8:38:c4:60:4a:65:28:49:14:32:3c:cc:6d:cd:34:

29:83:84:74:a7:2d:0e:75:1c:c2:52:58:1e:22:16:

12:d0:b4:8a:92

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

1A:61:60:4D:76:40:B8:BA:5D:A1:3C:60:BC:57:98:35:20:79:80:FC

X509v3 Authority Key Identifier:

keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22


```

Signature Algorithm: ecdsa-with-SHA256
30:66:02:31:00:9a:6d:fd:7d:ab:ae:54:9a:81:71:e6:bb:ad:
5a:2e:dc:1d:b3:8a:bf:ce:ee:71:4e:8f:d9:93:7f:a3:48:a1:
5c:17:cb:22:fa:8f:b3:e5:76:89:06:9f:96:47:dc:34:87:02:
31:00:e3:af:2a:8f:d6:8d:1f:3a:2b:ae:2f:97:b3:52:63:b6:
18:67:70:2c:93:2a:41:c0:e7:fa:93:20:09:4d:f4:bf:d0:11:
66:0f:48:56:01:1e:c3:be:37:4e:49:19:cf:c6

```

Assign an IP address to GigabitEthernet 2/0/1.

```
[RouterA] interface gigabitethernet 2/0/1
```

```
[RouterA-GigabitEthernet2/0/1] ip address 192.168.1.56 255.255.255.0
```

```
[RouterA-GigabitEthernet2/0/1] quit
```

3. Configure the Stelnet server:

Upload the server's certificate file **ssh-server-ecdsa256.p12** and the client's certificate file **ssh-client-ecdsa256.p12** to the Stelnet server through FTP or TFTP. (Details not shown.)

Create a PKI domain named **client256** for verifying the client's certificate and import the file of the client's certificate to this domain. (Details not shown.)

Create a PKI domain named **server256** for the server's certificate and import the file of the server's certificate to this domain. (Details not shown.)

Specify Suite B algorithms for algorithm negotiation.

```
<RouterB> system-view
```

```
[RouterB] ssh2 algorithm key-exchange ecdh-sha2-nistp256
```

```
[RouterB] ssh2 algorithm cipher aes128-gcm
```

```
[RouterB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384
```

Specify **server256** as the PKI domain of the server's certificate.

```
[RouterB] ssh server pki-domain server256
```

Enable the Stelnet server.

```
[RouterB] ssh server enable
```

Assign an IP address to GigabitEthernet 2/0/1.

```
[RouterB] interface gigabitethernet 2/0/1
```

```
[RouterB-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
```

```
[RouterB-GigabitEthernet2/0/1] quit
```

Set the authentication mode to AAA for user lines.

```
[RouterB] line vty 0 15
```

```
[RouterB-line-vty0-15] authentication-mode scheme
```

```
[RouterB-line-vty0-15] quit
```

Create a local device management user named **client001**. Authorize the user to use the **SSH** service and assign the **network-admin** user role to the user.

```
[RouterB] local-user client001 class manage
```

```
[RouterB-luser-manage-client001] service-type ssh
```

```
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
```

```
[RouterB-luser-manage-client001] quit
```

Create an SSH user named **client001**. Specify the authentication method **publickey** for the user and specify **client256** as the PKI domain for verifying the client's certificate.

```
[RouterB] ssh user client001 service-type stelnet authentication-type publickey
assign pki-domain client256
```

4. Establish an SSH connection to the Stelnet server **192.168.1.40** based on the 128-bit Suite B algorithms.

```

<RouterA> ssh2 192.168.1.40 suite-b 128-bit pki-domain client256 server-pki-domain
server256
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
Enter a character ~ and a dot to abort.

```

```

*****
*   Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP.           *
*   Without the owner's prior written consent,                                 *
*   no decompiling or reverse-engineering shall be allowed.                     *
*****

```

```

<RouterB>

```

SFTP configuration examples

Unless otherwise noted, devices in the configuration examples operate in non-FIPS mode.

When you configure SFTP on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as an SFTP server, only RSA key pairs are supported. Do not generate a DSA key pair on the SFTP server.

Password authentication enabled SFTP server configuration example

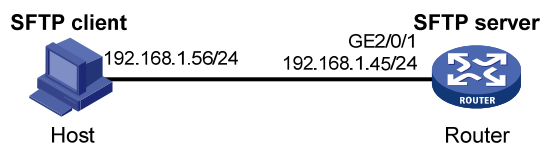
Network requirements

As shown in [Figure 128](#):

- The router acts as the SFTP server and uses password authentication.
- The username and password of the client are saved on the router.

Establish an SFTP connection between the host and the router, so you can log in to the router to manage and transfer files.

Figure 128 Network diagram



Configuration procedure

1. Configure the SFTP server:

```

# Generate RSA key pairs.

```

```

<Router> system-view

```

```

[Router] public-key local create rsa

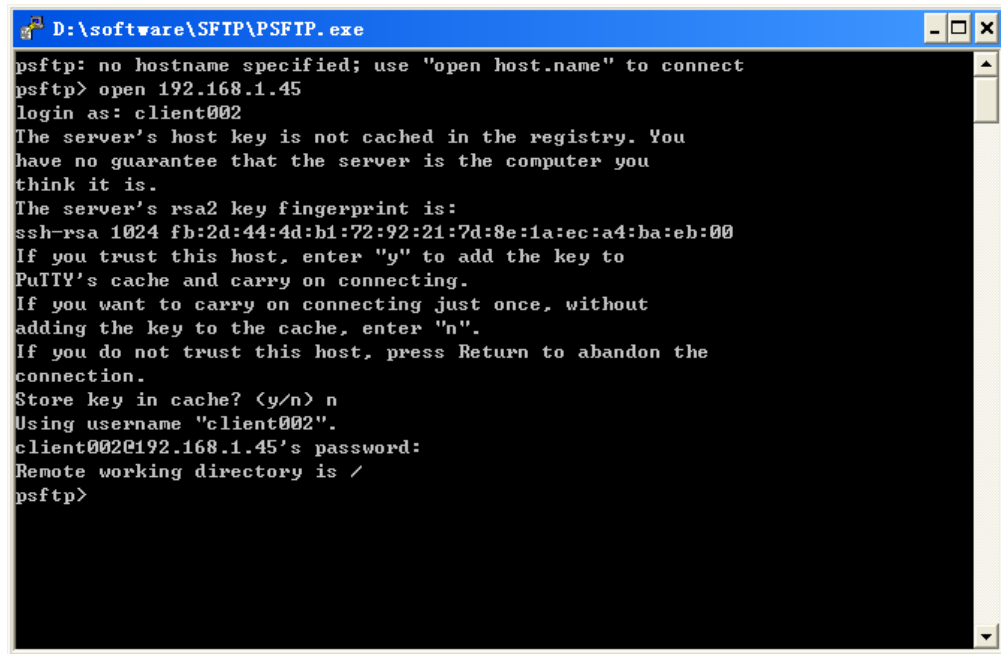
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

- a. Run the **psftp.exe** to launch the client interface shown in [Figure 129](#), and enter the following command:
open 192.168.1.45
- b. Enter username **client002** and password **aabbcc** as prompted to log in to the SFTP server.

Figure 129 SFTP client interface



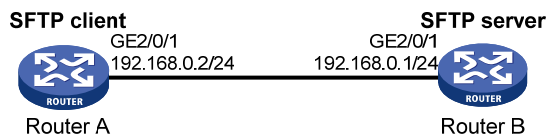
Publickey authentication enabled SFTP client configuration example

Network requirements

As shown in [Figure 130](#), Router B acts as the SFTP server, and it uses publickey authentication and the RSA public key algorithm.

Establish an SFTP connection between Router A and Router B, so you can log in to Router B to manage and transfer files.

Figure 130 Network diagram



Configuration procedure

In the server configuration, the client's host public key is required. Generate RSA key pairs on the client before configuring the SFTP server.

1. Configure the SFTP client:

Assign an IP address to GigabitEthernet 2/0/1.

```
<RouterA> system-view
```

```
[RouterA] interface gigabitethernet 2/0/1
```

```
[RouterA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
```



```
[RouterB-GigabitEthernet2/0/1] quit
# Import the peer public key from the file pubkey, and name it routerkey.
[RouterB] public-key peer routerkey import sshkey pubkey
# Create an SSH user named client001. Specify the service type as sftp and the authentication
method as publickey for the user. Assign the public key routerkey to the user.
[RouterB] ssh user client001 service-type sftp authentication-type publickey assign
publickey routerkey
# Create a local device management user named client001.
[RouterB] local-user client001 class manage
# Authorize the local user client001 to use the SSH service.
[RouterB-luser-manage-client001] service-type ssh
# Assign the network-admin user role and the working directory flash:/ to the local user
client001.
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
work-directory flash:/
[RouterB-luser-manage-client001] quit
```

3. Establish a connection between the SFTP client and the SFTP server:

Establish a connection to the SFTP server and enter SFTP client view.

```
<RouterA> sftp 192.168.0.1 identity-key rsa
```

```
Username: client001
```

```
Press CTRL+C to abort.
```

```
Connecting to 192.168.0.1 port 22.
```

```
The server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

```
sftp>
```

Display files under the current directory of the server, delete the file **z**, and verify the result.

```
sftp> dir -l
```

```
-rwxrwxrwx  1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone    nogroup        283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone    nogroup        225 Sep 01 06:55 pub
-rwxrwxrwx  1 noone    nogroup         0 Sep 01 08:00 z
```

```
sftp> delete z
```

```
Removing /z
```

```
sftp> dir -l
```

```
-rwxrwxrwx  1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone    nogroup        283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone    nogroup        225 Sep 01 06:55 pub
```

Add a directory **new1** and verify the result.

```
sftp> mkdir new1
```

```
sftp> dir -l
```

```
-rwxrwxrwx  1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone    nogroup        283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone    nogroup         0 Sep 01 06:22 new
```

```

-rwxrwxrwx  1 noone  nogroup      225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup        0 Sep 02 06:30 new1
# Rename the directory new1 to new2 and verify the result.
sftp> rename new1 new2
sftp> dir
-rwxrwxrwx  1 noone  nogroup    1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup    225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup    283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup        0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup    225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup        0 Sep 02 06:33 new2
# Download the pubkey2 file from the server and save it as a local file public.
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                100% 225      1.4KB/s   00:00
# Upload a local file pu to the server, save it as puk, and verify the result.
sftp> put pu puk
Uploading pu to / puk
sftp> dir
-rwxrwxrwx  1 noone  nogroup    1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup    225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup    283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup        0 Sep 01 06:22 new
drwxrwxrwx  1 noone  nogroup        0 Sep 02 06:33 new2
-rwxrwxrwx  1 noone  nogroup    283 Sep 02 06:35 pub
-rwxrwxrwx  1 noone  nogroup    283 Sep 02 06:36 puk
sftp>
# Exit SFTP client view.
sftp> quit
<RouterA>

```

SFTP configuration example based on 192-bit Suite B algorithms

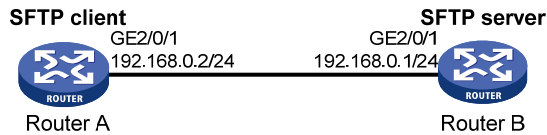
Network requirements

As shown in [Figure 131](#):

- Router A acts as an SFTP client (SSH2).
- Router B acts as the SFTP server (SSH2), and it uses publickey authentication.
- Router B uses the following algorithms for the algorithm negotiation with the SFTP client:
 - Key exchange algorithm **ecdh-sha2-nistp384**.
 - Encryption algorithm **aes256-gcm**.
 - Public key algorithm **x509v3-ecdsa-sha2-nistp384**.

Configure Router A to establish an SFTP connection to Router B based on the 192-bit Suite B algorithms. After the connection is established, you can log in to Router B to manage and transfer files.

Figure 131 Network diagram



Configuration procedure

1. Generate the client's certificate and the server's certificate. (Details not shown.)
You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.

In this example, the server's certificate file is **ssh-server-ecdsa384.p12** and the client's certificate file is **ssh-client-ecdsa384.p12**.

2. Configure the SFTP client:

NOTE:

You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE router as an SFTP client.

Upload the server's certificate file **ssh-server-ecdsa384.p12** and the client's certificate file **ssh-client-ecdsa384.p12** to the SFTP client through FTP or TFTP. (Details not shown.)

Create a PKI domain named **server384** for verifying the server's certificate and enter its view.

```
<RouterA> system-view
```

```
[RouterA] pki domain server384
```

Disable CRL checking.

```
[RouterA-pki-domain-server384] undo crl check enable
```

```
[RouterA-pki-domain-server384] quit
```

Import the local certificate file **ssh-server-ecdsa384.p12** to the PKI domain **server384**.

```
[RouterA] pki import domain server384 p12 local filename ssh-server-ecdsa384.p12
```

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name[default name: server384]:

Display information about local certificates in the PKI domain **server384**.

```
[RouterA] display pki certificate domain server384 local
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA

Validity

Not Before: Aug 20 10:08:41 2015 GMT

Not After : Aug 19 10:08:41 2016 GMT

Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=ssh server

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (384 bit)

pub:


```

04:4a:33:e5:99:8d:49:45:a7:a3:24:7b:32:6a:ed:
b6:36:e1:4d:cc:8c:05:22:f4:3a:7c:5d:b7:be:d1:
e6:9e:f0:ce:95:39:ca:fd:a0:86:cd:54:ab:49:60:
10:be:67:9f:90:3a:18:e2:7d:d9:5f:72:27:09:e7:
bf:7e:64:0a:59:bb:b3:7d:ae:88:14:94:45:b9:34:
d2:f3:93:e1:ba:b4:50:15:eb:e5:45:24:31:10:c7:
07:01:f9:dc:a5:6f:81
ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    10:16:64:2C:DA:C1:D1:29:CD:C0:74:40:A9:70:BD:62:8A:BB:F4:D5
  X509v3 Authority Key Identifier:
    keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

Signature Algorithm: ecdsa-with-SHA384
30:65:02:31:00:80:50:7a:4f:c5:cd:6a:c3:57:13:7f:e9:da:
c1:72:7f:45:30:17:c2:a7:d3:ec:73:3d:5f:4d:e3:96:f6:a3:
33:fb:e4:b9:ff:47:f1:af:9d:e3:03:d2:24:53:40:09:5b:02:
30:45:d1:bf:51:fd:da:22:11:90:03:f9:d4:05:ec:d6:7c:41:
fc:9d:a1:fd:5b:8c:73:f8:b6:4c:c3:41:f7:c6:7f:2f:05:2d:
37:f8:52:52:26:99:28:97:ac:6e:f9:c7:01

# Create a PKI domain named client384 for the client's certificate and enter its view.
[RouterA] pki domain client384

# Disable CRL checking.
[RouterA-pki-domain-client384] undo crl check enable
[RouterA-pki-domain-client384] quit

# Import the local certificate file ssh-client-ecdsa384.p12 to the PKI domain client384.
[RouterA] pki import domain client384 p12 local filename ssh-client-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client384]:

# Display information about local certificates in the PKI domain client384.
[RouterA]display pki certificate domain client384 local
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
  Signature Algorithm: ecdsa-with-SHA384
  Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
  Validity
    Not Before: Aug 20 10:10:59 2015 GMT
    Not After : Aug 19 10:10:59 2016 GMT

```

```

Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=ssh client
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
    Public-Key: (384 bit)
      pub:
        04:85:7c:8b:f4:7a:36:bf:74:f6:7c:72:f9:08:69:
        d0:b9:ac:89:98:17:c9:fc:89:94:43:da:9a:a6:89:
        41:d3:72:24:9b:9a:29:a8:d1:ba:b4:e5:77:ba:fc:
        df:ae:c6:dd:46:72:ab:bc:d1:7f:18:7d:54:88:f6:
        b4:06:54:7e:e7:4d:49:b4:07:dc:30:54:4b:b6:5b:
        01:10:51:6b:0c:6d:a3:b1:4b:c9:d9:6c:d6:be:13:
        91:70:31:2a:92:00:76
      ASN1 OID: secp384r1
      NIST CURVE: P-384
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      BD:5F:8E:4F:7B:FE:74:03:5A:D1:94:DB:CA:A7:82:D6:F7:78:A1:B0
    X509v3 Authority Key Identifier:
      keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

```

```

Signature Algorithm: ecdsa-with-SHA384
30:66:02:31:00:d2:06:fa:2c:0b:0d:f0:81:90:01:c3:3d:bf:
97:b3:79:d8:25:a0:e2:0e:ed:00:c9:48:3e:c9:71:43:c9:b4:
2a:a6:0a:27:80:9e:d4:0f:f2:db:db:5b:40:b1:a9:0a:e4:02:
31:00:ee:00:e1:07:c0:2f:12:3f:88:ea:fe:19:05:ef:56:ca:
33:71:75:5e:11:c9:a6:51:4b:3e:7c:eb:2a:4d:87:2b:71:7c:
30:64:fe:14:ce:06:d5:0a:e2:cf:9a:69:19:ff

```

Assign an IP address to GigabitEthernet 2/0/1.

```

[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet2/0/1] quit

```

3. Configure the SFTP server:

```

# Upload the server's certificate file ssh-server-ecdsa384.p12 and the client's certificate file
ssh-client-ecdsa384.p12 to the SFTP server through FTP or TFTP. (Details not shown.)
# Create a PKI domain named client384 for verifying the client's certificate and import the file of
the client's certificate to this domain. (Details not shown.)
# Create a PKI domain named server384 for the server's certificate and import the file of the
server's certificate to this domain. (Details not shown.)
# Specify Suite B algorithms for algorithm negotiation.
[RouterB] ssh2 algorithm key-exchange ecdh-sha2-nistp384
[RouterB] ssh2 algorithm cipher aes256-gcm
[RouterB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp384
# Specify server384 as the PKI domain of the server's certificate.
[RouterB] ssh server pki-domain server384

```

```

# Enable the SFTP server.
[RouterB] sftp server enable

# Assign an IP address to GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet2/0/1] quit

# Set the authentication mode to AAA for user lines.
[RouterB] line vty 0 15
[RouterB-line-vty0-15] authentication-mode scheme
[RouterB-line-vty0-15] quit

# Create a local device management user named client001. Authorize the user to use the SSH
service and assign the network-admin user role to the user.
[RouterB] local-user client001 class manage
[RouterB-luser-manage-client001] service-type ssh
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
[RouterB-luser-manage-client001] quit

# Create an SSH user named client001. Specify the authentication method publickey for the
user and specify client384 as the PKI domain for verifying the client's certificate.
[RouterB] ssh user client001 service-type sftp authentication-type publickey assign
pki-domain client384

```

4. Establish an SFTP connection to the SFTP server **192.168.0.1** based on the 192-bit Suite B algorithms.

```

<RouterA> sftp 192.168.0.1 suite-b 192-bit pki-domain client384 server-pki-domain
server384
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
sftp>

```

SCP configuration examples

Unless otherwise noted, devices in the configuration examples operate in non-FIPS mode.

When you configure SCP on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as an SCP server, only RSA key pairs are supported. Do not generate a DSA key pair on the SCP server.

SCP configuration example with password authentication

Network requirements

As shown in [Figure 132](#):

- Router B uses the password authentication method.
- The client's username and password are saved on Router B.

Establish an SCP connection between Router A and Router B, so you can log in to Router B to transfer files.

The diagram shows a network topology for SCP. On the left is Router A, labeled "SCP client". It has a GE2/0/1 interface connected to the network 192.168.0.2/24. On the right is Router B, labeled "SCP server". It has a GE2/0/1 interface connected to the network 192.168.0.1/24. A single line represents the connection between the two routers.

1. Configure the SCP server:

```
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
```

- ```
[RouterB-luser-manage-client001] quit
Create an SSH user named client001. Specify the service type as scp and the authentication
method password for the user.
[RouterB] ssh user client001 service-type scp authentication-type password
```
- Assign an IP address to GigabitEthernet 2/0/1 on the SCP client.

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] quit
```
  - Connect to the SCP server, download the file **remote.bin** from the server, and save it locally to the file **local.bin**.

```
<RouterA> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
remote.bin 100% 2875 2.8KB/s 00:00
```

## SCP configuration example based on Suite B algorithms

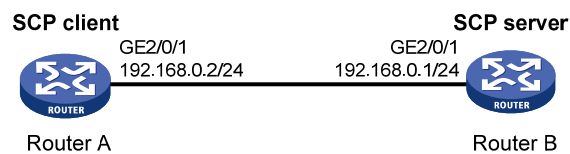
### Network requirements

As shown in [Figure 133](#):

- Router A acts as an SCP client (SSH2).
- Router B acts as the SCP server (SSH2), and it uses publickey authentication.
- Router B uses the following algorithms for the algorithm negotiation with the SCP client:
  - Key exchange algorithms **ecdh-sha2-nistp256** and **ecdh-sha2-nistp384**.
  - Encryption algorithms **aes128-gcm** and **aes256-gcm**.
  - Public key algorithms **x509v3-ecdsa-sha2-nistp256** and **x509v3-ecdsa-sha2-nistp384**.

Configure Router A to establish an SCP connection to Router B based on Suite B algorithms. After the connection is established, you can log in to Router B to transfer files.

**Figure 133 Network diagram**



### Configuration procedure

- Generate the client's certificates and the server's certificates. (Details not shown.)  
You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.  
In this example, the server's certificate files are **ssh-server-ecdsa256.p12** and **ssh-server-ecdsa384.p12**. The client's certificate files are **ssh-client-ecdsa256.p12** and **ssh-client-ecdsa384.p12**.

## 2. Configure the SCP client:

---

### NOTE:

You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE router as an SCP client.

---

```
Upload the server's certificate files (ssh-server-ecdsa256.p12 and
ssh-server-ecdsa384.p12) and the client's certificate files (ssh-client-ecdsa256.p12 and
ssh-client-ecdsa384.p12) to the SCP client through FTP or TFTP. (Details not shown.)
Create a PKI domain named server256 for verifying the server's certificate ecdsa256 and
enter its view.
<RouterA> system-view
[RouterA] pki domain server256
Disable CRL checking.
[RouterA-pki-domain-server256] undo crl check enable
[RouterA-pki-domain-server256] quit
Import the local certificate file ssh-server-ecdsa256.p12 to the PKI domain server256.
[RouterA] pki import domain server256 p12 local filename ssh-server-ecdsa256.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: server256]:
Display information about local certificates in the PKI domain server256.
[RouterA] display pki certificate domain server256 local
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 3 (0x3)
 Signature Algorithm: ecdsa-with-SHA256
 Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
 Validity
 Not Before: Aug 21 08:39:51 2015 GMT
 Not After : Aug 20 08:39:51 2016 GMT
 Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=SSH Server secp256
 Subject Public Key Info:
 Public Key Algorithm: id-ecPublicKey
 Public-Key: (256 bit)
 pub:
 04:a2:b4:b4:66:1e:3b:d5:50:50:0e:55:19:8d:52:
 6d:47:8c:3d:3d:96:75:88:2f:9a:ba:a2:a7:f9:ef:
 0a:a9:20:b7:b6:6a:90:0e:f8:c6:de:15:a2:23:81:
 3c:9e:a2:b7:83:87:b9:ad:28:c8:2a:5e:58:11:8e:
 c7:61:4a:52:51
 ASN1 OID: prime256v1
 NIST CURVE: P-256
 X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Comment:
```

```

 OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
 08:C1:F1:AA:97:45:19:6A:DA:4A:F2:87:A1:1A:E8:30:BD:31:30:D7
X509v3 Authority Key Identifier:
 keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

Signature Algorithm: ecdsa-with-SHA256
 30:65:02:31:00:a9:16:e9:c1:76:f0:32:fc:4b:f9:8f:b6:7f:
 31:a0:9f:de:a7:cc:33:29:27:2c:71:2e:f9:0d:74:cb:25:c9:
 00:d2:52:18:7f:58:3f:cc:7e:8b:d3:42:65:00:cb:63:f8:02:
 30:01:a2:f6:a1:51:04:1c:61:78:f6:6b:7e:f9:f9:42:8d:7c:
 a7:bb:47:7c:2a:85:67:0d:81:12:0b:02:98:bc:06:1f:c1:3c:
 9b:c2:1b:4c:44:38:5a:14:b2:48:63:02:2b

Create a PKI domain named client256 for the client's certificate ecdsa256 and enter its view.
[RouterA] pki domain client256
Disable CRL checking.
[RouterA-pki-domain-client256] undo crl check enable
[RouterA-pki-domain-client256] quit
Import the local certificate file ssh-client-ecdsa256.p12 to the PKI domain client256.
[RouterA] pki import domain client256 p12 local filename ssh-client-ecdsa256.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client256]:
Display information about local certificates in the PKI domain client256.
[RouterA] display pki certificate domain client256 local
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 4 (0x4)
 Signature Algorithm: ecdsa-with-SHA256
 Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
 Validity
 Not Before: Aug 21 08:41:09 2015 GMT
 Not After : Aug 20 08:41:09 2016 GMT
 Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=SSH Client secp256
 Subject Public Key Info:
 Public Key Algorithm: id-ecPublicKey
 Public-Key: (256 bit)
 pub:
 04:da:e2:26:45:87:7a:63:20:e7:ca:7f:82:19:f5:
 96:88:3e:25:46:f8:2f:9a:4c:70:61:35:db:e4:39:
 b8:38:c4:60:4a:65:28:49:14:32:3c:cc:6d:cd:34:
 29:83:84:74:a7:2d:0e:75:1c:c2:52:58:1e:22:16:
 12:d0:b4:8a:92
 ASN1 OID: prime256v1
 NIST CURVE: P-256
 X509v3 extensions:

```

```

X509v3 Basic Constraints:
 CA:FALSE
Netscape Comment:
 OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
 1A:61:60:4D:76:40:B8:BA:5D:A1:3C:60:BC:57:98:35:20:79:80:FC
X509v3 Authority Key Identifier:
 keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

Signature Algorithm: ecdsa-with-SHA256
 30:66:02:31:00:9a:6d:fd:7d:ab:ae:54:9a:81:71:e6:bb:ad:
 5a:2e:dc:1d:b3:8a:bf:ce:ee:71:4e:8f:d9:93:7f:a3:48:a1:
 5c:17:cb:22:fa:8f:b3:e5:76:89:06:9f:96:47:dc:34:87:02:
 31:00:e3:af:2a:8f:d6:8d:1f:3a:2b:ae:2f:97:b3:52:63:b6:
 18:67:70:2c:93:2a:41:c0:e7:fa:93:20:09:4d:f4:bf:d0:11:
 66:0f:48:56:01:1e:c3:be:37:4e:49:19:cf:c6

Create a PKI domain named server384 for verifying the server's certificate ecdsa384 and
enter its view.
[RouterA] pki domain server384
Disable CRL checking.
[RouterA-pki-domain-server384] undo crl check enable
[RouterA-pki-domain-server384] quit
Import the local certificate file ssh-server-ecdsa384.p12 to the PKI domain server384.
[RouterA] pki import domain server384 p12 local filename ssh-server-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: server384]:
Display information about local certificates in the PKI domain server384.
[RouterA] display pki certificate domain server384 local
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 1 (0x1)
 Signature Algorithm: ecdsa-with-SHA384
 Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
 Validity
 Not Before: Aug 20 10:08:41 2015 GMT
 Not After : Aug 19 10:08:41 2016 GMT
 Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=ssh server
 Subject Public Key Info:
 Public Key Algorithm: id-ecPublicKey
 Public-Key: (384 bit)
 pub:
 04:4a:33:e5:99:8d:49:45:a7:a3:24:7b:32:6a:ed:
 b6:36:e1:4d:cc:8c:05:22:f4:3a:7c:5d:b7:be:d1:
 e6:9e:f0:ce:95:39:ca:fd:a0:86:cd:54:ab:49:60:
 10:be:67:9f:90:3a:18:e2:7d:d9:5f:72:27:09:e7:

```



```

 bf:7e:64:0a:59:bb:b3:7d:ae:88:14:94:45:b9:34:
 d2:f3:93:e1:ba:b4:50:15:eb:e5:45:24:31:10:c7:
 07:01:f9:dc:a5:6f:81
ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Comment:
 OpenSSL Generated Certificate
 X509v3 Subject Key Identifier:
 10:16:64:2C:DA:C1:D1:29:CD:C0:74:40:A9:70:BD:62:8A:BB:F4:D5
 X509v3 Authority Key Identifier:
 keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

Signature Algorithm: ecdsa-with-SHA384
 30:65:02:31:00:80:50:7a:4f:c5:cd:6a:c3:57:13:7f:e9:da:
 c1:72:7f:45:30:17:c2:a7:d3:ec:73:3d:5f:4d:e3:96:f6:a3:
 33:fb:e4:b9:ff:47:f1:af:9d:e3:03:d2:24:53:40:09:5b:02:
 30:45:d1:bf:51:fd:da:22:11:90:03:f9:d4:05:ec:d6:7c:41:
 fc:9d:a1:fd:5b:8c:73:f8:b6:4c:c3:41:f7:c6:7f:2f:05:2d:
 37:f8:52:52:26:99:28:97:ac:6e:f9:c7:01

Create a PKI domain named client384 for the client's certificate ecdsa384 and enter its view.
[RouterA] pki domain client384
Disable CRL checking.
[RouterA-pki-domain-client384] undo crl check enable
[RouterA-pki-domain-client384] quit
Import the local certificate file ssh-client-ecdsa384.p12 to the PKI domain client384.
[RouterA] pki import domain client384 p12 local filename ssh-client-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client384]:
Display information about local certificates in the PKI domain client384.
[RouterA] display pki certificate domain client384 local
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 2 (0x2)
 Signature Algorithm: ecdsa-with-SHA384
 Issuer: C=CN, ST=aaa, L=bbb, O=ccc, OU=Software, CN=SuiteB CA
 Validity
 Not Before: Aug 20 10:10:59 2015 GMT
 Not After : Aug 19 10:10:59 2016 GMT
 Subject: C=CN, ST=aaa, O=ccc, OU=Software, CN=ssh client
 Subject Public Key Info:
 Public Key Algorithm: id-ecPublicKey
 Public-Key: (384 bit)

```

```

pub:
 04:85:7c:8b:f4:7a:36:bf:74:f6:7c:72:f9:08:69:
 d0:b9:ac:89:98:17:c9:fc:89:94:43:da:9a:a6:89:
 41:d3:72:24:9b:9a:29:a8:d1:ba:b4:e5:77:ba:fc:
 df:ae:c6:dd:46:72:ab:bc:d1:7f:18:7d:54:88:f6:
 b4:06:54:7e:e7:4d:49:b4:07:dc:30:54:4b:b6:5b:
 01:10:51:6b:0c:6d:a3:b1:4b:c9:d9:6c:d6:be:13:
 91:70:31:2a:92:00:76
ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Comment:
 OpenSSL Generated Certificate
 X509v3 Subject Key Identifier:
 BD:5F:8E:4F:7B:FE:74:03:5A:D1:94:DB:CA:A7:82:D6:F7:78:A1:B0
 X509v3 Authority Key Identifier:
 keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

```

```

Signature Algorithm: ecdsa-with-SHA384
 30:66:02:31:00:d2:06:fa:2c:0b:0d:f0:81:90:01:c3:3d:bf:
 97:b3:79:d8:25:a0:e2:0e:ed:00:c9:48:3e:c9:71:43:c9:b4:
 2a:a6:0a:27:80:9e:d4:0f:f2:db:db:5b:40:b1:a9:0a:e4:02:
 31:00:ee:00:e1:07:c0:2f:12:3f:88:ea:fe:19:05:ef:56:ca:
 33:71:75:5e:11:c9:a6:51:4b:3e:7c:eb:2a:4d:87:2b:71:7c:
 30:64:fe:14:ce:06:d5:0a:e2:cf:9a:69:19:ff

```

# Assign an IP address to GigabitEthernet 2/0/1.

```

[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] quit

```

### 3. Configure the SCP server:

```

Upload the server's certificate files (ssh-server-ecdsa256.p12 and
ssh-server-ecdsa384.p12) and the client's certificate files (ssh-client-ecdsa256.p12 and
ssh-client-ecdsa384.p12) to the SCP server through FTP or TFTP. (Details not shown.)
Create a PKI domain named client256 for verifying the client's certificate ecdsa256 and
import the file of this certificate to this domain. Create a PKI domain named server256 for the
server's certificate ecdsa256 and import the file of this certificate to this domain. (Details not
shown.)
Create a PKI domain named client384 for verifying the client's certificate ecdsa384 and
import the file of this certificate to this domain. Create a PKI domain named server384 for the
server's certificate ecdsa384 and import the file of this certificate to this domain. (Details not
shown.)
Specify Suite B algorithms for algorithm negotiation.
<RouterB> system-view
[RouterB] ssh2 algorithm key-exchange ecdh-sha2-nistp256 ecdh-sha2-nistp384
[RouterB] ssh2 algorithm cipher aes128-gcm aes256-gcm

```

```

[RouterB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384
Enable the SCP server.
[RouterB] scp server enable
Assign an IP address to GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet2/0/1] quit
Set the authentication mode to AAA for user lines.
[RouterB] line vty 0 15
[RouterB-line-vty0-15] authentication-mode scheme
[RouterB-line-vty0-15] quit
Create a local device management user named client001. Authorize the user to use the SSH
service and assign the network-admin user role to the user.
[RouterB] local-user client001 class manage
[RouterB-luser-manage-client001] service-type ssh
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
[RouterB-luser-manage-client001] quit
Create a local device management user named client002. Authorize the user to use the SSH
service and assign the network-admin user role to the user.
[RouterB] local-user client002 class manage
[RouterB-luser-manage-client002] service-type ssh
[RouterB-luser-manage-client002] authorization-attribute user-role network-admin
[RouterB-luser-manage-client002] quit

```

#### 4. Establish an SCP connection to the SCP server **192.168.0.1**:

- Based on the 128-bit Suite B algorithms:
  - # Specify **server256** as the PKI domain of the server's certificate.
  - [RouterB] ssh server pki-domain server256
  - # Create an SSH user named **client001**. Specify the authentication method **publickey** for the user and specify **client256** as the PKI domain for verifying the client's certificate.
  - [RouterB] ssh user client001 service-type sftp authentication-type publickey assign pki-domain client256
  - # Establish an SCP connection to the SCP server **192.168.0.1** based on the 128-bit Suite B algorithms.

```

<RouterA> scp 192.168.0.1 get src.cfg suite-b 128-bit pki-domain client256
server-pki
-domain server256
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
src.cfg 100% 4814 4.7KB/s 00:00
<RouterA>

```
- Based on the 192-bit Suite B algorithms:
  - # Specify **server384** as the PKI domain of the server's certificate.
  - [RouterB] ssh server pki-domain server384
  - # Create an SSH user named **client002**. Specify the authentication method **publickey** for the user and specify **client384** as the PKI domain for verifying the client's certificate.
  - [RouterB] ssh user client002 service-type scp authentication-type publickey assign pki-domain client384

```
Establish an SCP connection to the SCP server 192.168.0.1 based on the 192-bit Suite B
algorithms.
<RouterA> scp 192.168.0.1 get src.cfg suite-b 192-bit pki-domain client384
server-pki
-domain server384
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
src.cfg 100% 4814 4.7KB/s 00:00
<RouterA>
```

## NETCONF over SSH configuration example

Unless otherwise noted, devices in the configuration examples are in non-FIPS mode.

When you configure NETCONF-over-SSH on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as a NETCONF-over-SSH server, only RSA key pairs are supported. Do not generate a DSA key pair on the NETCONF-over-SSH server.

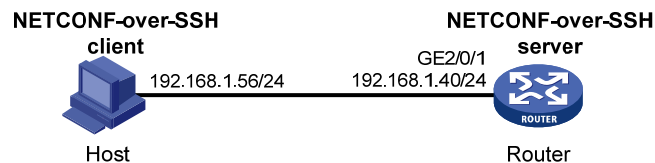
## Network requirements

As shown in [Figure 134](#):

- The router uses local password authentication.
- The client's username and password are saved on the router.

Establish a NETCONF-over-SSH connection between the host and the router, so that you can log in to the router to perform NETCONF operations.

**Figure 134 Network diagram**



## Configuration procedure

```
Generate RSA key pairs.
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....++++++
.....++++++
..++++++
```

```

.....+++++++
Create the key pair successfully.
Generate a DSA key pair.
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.+++++++*
.....+.....+.....+.....+
...+.....+.....+...+
Create the key pair successfully.
Enable NETCONF over SSH.
[Router] netconf ssh server enable

Assign an IP address to GigabitEthernet 2/0/1. The client uses this address as the destination for
NETCONF-over-SSH connection.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip address 192.168.1.40 255.255.255.0
[Router-GigabitEthernet2/0/1] quit

Set the authentication mode to AAA for the user lines.
[Router] line vty 0 15
[Router-line-vty0-15] authentication-mode scheme
[Router-line-vty0-15] quit

Create a local device management user named client001.
[Router] local-user client001 class manage

Set the password to aabbcc in plain text for the local user client001.
[Router-luser-manage-client001] password simple aabbcc

Authorize the local user client001 to use the SSH service.
[Router-luser-manage-client001] service-type ssh

Assign the network-admin user role to the local user client001.
[Router-luser-manage-client001] authorization-attribute user-role network-admin
[Router-luser-manage-client001] quit

Create an SSH user named client001. Specify the service type as NETCONF and the
authentication method as password for the user.
[Router] ssh user client001 service-type netconf authentication-type password

```

## Verifying the configuration

```

Verify that you can perform NETCONF operations after logging in to the router. (Details not shown.)

```

# Configuring SSL

## Overview

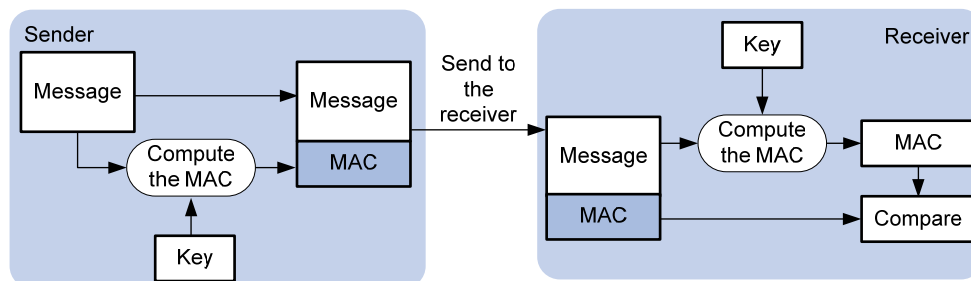
Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security for TCP-based application layer protocols such as HTTP. SSL has been widely used in applications such as e-business and online banking to provide secure data transmission over the Internet.

## SSL security services

SSL provides the following security services:

- **Privacy**—SSL uses a symmetric encryption algorithm to encrypt data. It uses the asymmetric key algorithm of RSA to encrypt the key used by the symmetric encryption algorithm. For more information about RSA, see "[Managing public keys](#)."
- **Authentication**—SSL uses certificate-based digital signatures to authenticate the SSL server and client. The SSL server and client obtain digital certificates through PKI. For more information about PKI and digital certificates, see "[Configuring PKI](#)."
- **Integrity**—SSL uses the message authentication code (MAC) to verify message integrity. It uses a MAC algorithm and a key to transform a message of any length to a fixed-length message. Any change to the original message will result in a change to the calculated fixed-length message. As shown in [Figure 135](#), the message integrity verification process is as follows:
  - a. The sender uses a MAC algorithm and a key to calculate a MAC value for a message. Then, it appends the MAC value to the message and sends the message to the receiver.
  - b. The receiver uses the same key and MAC algorithm to calculate a MAC value for the received message, and compares it with the MAC value appended to the message.
  - c. If the two MAC values match, the receiver considers the message intact. Otherwise, the receiver considers that the message was tampered with and it discards the message.

**Figure 135 MAC algorithm diagram**

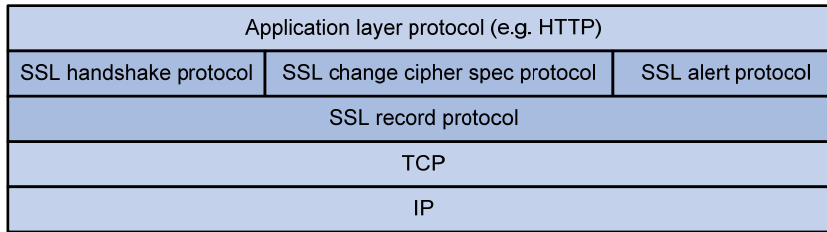


## SSL protocol stack

The SSL protocol stack includes the following protocols:

- SSL record protocol at the lower layer.
- SSL handshake protocol, SSL change cipher spec protocol, and SSL alert protocol at the upper layer.

**Figure 136 SSL protocol stack**



The following describes the major functions of SSL protocols:

- **SSL record protocol**—Fragments data received from the upper layer, computes and adds MAC to the data, and encrypts the data.
- **SSL handshake protocol**—Negotiates the cipher suite used for secure communication, authenticates the server and client, and securely exchanges the keys between the server and client. The cipher suite that needs to be negotiated includes the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm.
- **SSL change cipher spec protocol**—Notifies the receiver that subsequent packets are to be protected based on the negotiated cipher suite and key.
- **SSL alert protocol**—Sends alert messages to the receiving party. An alert message contains the alert severity level and a description.

## FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "[Configuring FIPS](#)") and non-FIPS mode.

## SSL configuration task list

| Tasks at a glance                                | Remarks                                            |
|--------------------------------------------------|----------------------------------------------------|
| <a href="#">Configuring an SSL server policy</a> | Perform this configuration task on the SSL server. |
| <a href="#">Configuring an SSL client policy</a> | Perform this configuration task on the SSL client. |

## Configuring an SSL server policy

An SSL server policy is a set of SSL parameters used by the SSL server. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

SSL protocol versions include SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. By default, the SSL server can communicate with clients running all SSL protocol versions. When the server receives an SSL 2.0 Client Hello message from a client, it notifies the client to use a later version for communication.

To configure an SSL server policy:

| Step                               | Command                                     | Remarks                   |
|------------------------------------|---------------------------------------------|---------------------------|
| 1. Enter system view.              | <b>system-view</b>                          | N/A                       |
| 2. Create an SSL server policy and | <b>ssl server-policy</b> <i>policy-name</i> | By default, no SSL server |

| Step                                                                                                    | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Remarks                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enter its view.                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | policies exist on the device.                                                                                                                                                                                                                                                                                                          |
| 3. (Optional.) Specify a PKI domain for the SSL server policy.                                          | <b>pki-domain</b> <i>domain-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <p>By default, no PKI domain is specified for an SSL server policy.</p> <p>If SSL server authentication is required, you must specify a PKI domain and request a local certificate for the SSL server in the domain.</p> <p>For information about how to create and configure a PKI domain, see "<a href="#">Configuring PKI</a>."</p> |
| 4. Specify the cipher suites that the SSL server policy supports.                                       | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/> <b>ciphersuite</b><br/> { <b>dhe_rsa_aes_128_cbc_sha</b>  <br/> <b>dhe_rsa_aes_128_cbc_sha256</b>  <br/> <b>dhe_rsa_aes_256_cbc_sha</b>  <br/> <b>dhe_rsa_aes_256_cbc_sha256</b>  <br/> <b>ecdhe_rsa_aes_128_cbc_sha256</b>  <br/> <b>ecdhe_rsa_aes_256_cbc_sha384</b>  <br/> <b>ecdhe_rsa_aes_128_gcm_sha256</b>  <br/> <b>ecdhe_rsa_aes_256_gcm_sha384</b>  <br/> <b>ecdhe_ecdsa_aes_128_cbc_sha256</b>  <br/> <b>ecdhe_ecdsa_aes_256_cbc_sha384</b>  <br/> <b>ecdhe_ecdsa_aes_128_gcm_sha256</b>  <br/> <b>ecdhe_ecdsa_aes_256_gcm_sha384</b>  <br/> <b>exp_rsa_des_cbc_sha</b>  <br/> <b>exp_rsa_rc2_md5</b>   <b>exp_rsa_rc4_md5</b>  <br/> <b>rsa_3des_edc_cbc_sha</b>  <br/> <b>rsa_aes_128_cbc_sha</b>  <br/> <b>rsa_aes_128_cbc_sha256</b>  <br/> <b>rsa_aes_256_cbc_sha</b>  <br/> <b>rsa_aes_256_cbc_sha256</b>  <br/> <b>rsa_des_cbc_sha</b>   <b>rsa_rc4_128_md5</b>  <br/> <b>rsa_rc4_128_sha</b> } * </li> <li>In FIPS mode:<br/> <b>ciphersuite</b><br/> { <b>ecdhe_rsa_aes_128_cbc_sha256</b>  <br/> <b>ecdhe_rsa_aes_256_cbc_sha384</b>  <br/> <b>ecdhe_rsa_aes_128_gcm_sha256</b>  <br/> <b>ecdhe_rsa_aes_256_gcm_sha384</b>  <br/> <b>ecdhe_ecdsa_aes_128_cbc_sha256</b>  <br/> <b>ecdhe_ecdsa_aes_256_cbc_sha384</b>  <br/> <b>ecdhe_ecdsa_aes_128_gcm_sha256</b>  <br/> <b>ecdhe_ecdsa_aes_256_gcm_sha384</b>  <br/> <b>rsa_aes_128_cbc_sha</b>  <br/> <b>rsa_aes_128_cbc_sha256</b>  <br/> <b>rsa_aes_256_cbc_sha</b>  <br/> <b>rsa_aes_256_cbc_sha256</b> } * </li> </ul> | By default, an SSL server policy supports all cipher suites.                                                                                                                                                                                                                                                                           |
| 5. Set the maximum number of sessions that the SSL server can cache and the session cache timeout time. | <b>session</b> { <b>cache-size</b> <i>size</i>   <b>timeout</b> <i>time</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | By default, the SSL server can cache a maximum of 500 sessions, and the session cache timeout time is 3600 seconds.                                                                                                                                                                                                                    |



| Step                                                                   | Command                                    | Remarks                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6. (Optional.) Enable mandatory or optional SSL client authentication. | <b>client-verify { enable   optional }</b> | By default, SSL client authentication is disabled. The SSL server does not perform digital certificate-based authentication on SSL clients.<br><br>When authenticating a client by using the digital certificate, the SSL server verifies the certificate chain presented by the client. It also checks that the certificates in the certificate chain (except the root CA certificate) are not revoked. |

## Configuring an SSL client policy

An SSL client policy is a set of SSL parameters that the client uses to establish a connection to the server. An SSL client policy takes effect only after it is associated with an application such as DDNS. For information about DDNS, see *Layer 3—IP Services Configuration Guide*.

To configure an SSL client policy:

| Step                                                             | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Remarks                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                            | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | N/A                                                                                                                                                                                                                                                                                                                                   |
| 2. Create an SSL client policy and enter its view.               | <b>ssl client-policy</b> <i>policy-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | By default, no SSL client policies exist on the device.                                                                                                                                                                                                                                                                               |
| 3. (Optional.) Specify a PKI domain for the SSL client policy.   | <b>pki-domain</b> <i>domain-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | By default, no PKI domain is specified for an SSL client policy.<br><br>If SSL client authentication is required, you must specify a PKI domain and request a local certificate for the SSL client in the PKI domain.<br><br>For information about how to create and configure a PKI domain, see " <a href="#">Configuring PKI</a> ." |
| 4. Specify the preferred cipher suite for the SSL client policy. | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/> <b>prefer-cipher</b><br/> { <b>dhe_rsa_aes_128_cbc_sha</b>   <b>dhe_rsa_aes_128_cbc_sha256</b>   <b>dhe_rsa_aes_256_cbc_sha</b>   <b>dhe_rsa_aes_256_cbc_sha256</b>   <b>ecdhe_rsa_aes_128_cbc_sha256</b>   <b>ecdhe_rsa_aes_256_cbc_sha384</b>   <b>ecdhe_rsa_aes_128_gcm_sha256</b>   <b>ecdhe_rsa_aes_256_gcm_sha384</b>   <b>ecdhe_ecdsa_aes_128_cbc_sha256</b>   <b>ecdhe_ecdsa_aes_256_cbc_sha384</b>   <b>ecdhe_ecdsa_aes_128_gcm_sha256</b>   <b>ecdhe_ecdsa_aes_256_gcm_sha384</b>   <b>exp_rsa_des_cbc_sha</b>   <b>exp_rsa_rc2_md5</b>   <b>exp_rsa_rc4_md5</b>   <b>rsa_3des_edc_cbc_sha</b>   <b>rsa_aes_128_cbc_sha</b>   </li> </ul> | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/>The default preferred cipher suite is <b>rsa_rc4_128_md5</b>.</li> <li>In FIPS mode:<br/>The default preferred cipher suite is <b>sa_aes_128_cbc_sha</b>.</li> </ul>                                                                                                     |

| Step                                                                           | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Remarks                                                                                                                                               |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                | <pre>rsa_aes_128_cbc_sha256   rsa_aes_256_cbc_sha   rsa_aes_256_cbc_sha256   rsa_des_cbc_sha   rsa_rc4_128_md5   rsa_rc4_128_sha }</pre> <ul style="list-style-type: none"> <li>In FIPS mode:<br/> <pre>prefer-cipher { ecdhe_rsa_aes_128_cbc_sha256   ecdhe_rsa_aes_256_cbc_sha384   ecdhe_rsa_aes_128_gcm_sha256   ecdhe_rsa_aes_256_gcm_sha384   ecdhe_ecdsa_aes_128_cbc_sha256   ecdhe_ecdsa_aes_256_cbc_sha384   ecdhe_ecdsa_aes_128_gcm_sha256   ecdhe_ecdsa_aes_256_gcm_sha384   rsa_aes_128_cbc_sha   rsa_aes_128_cbc_sha256   rsa_aes_256_cbc_sha   rsa_aes_256_cbc_sha256 }</pre> </li> </ul> |                                                                                                                                                       |
| 5. Specify the SSL protocol version for the SSL client policy.                 | <ul style="list-style-type: none"> <li>In non-FIPS mode:<br/> <pre>version { ssl3.0   tls1.0   tls1.1   tls1.2 }</pre> </li> <li>In FIPS mode:<br/> <pre>version { tls1.0   tls1.1   tls1.2 }</pre> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                         | <p>By default, an SSL client policy uses TLS 1.0.</p> <p>As a best practice to ensure security, do not specify SSL 3.0 for the SSL client policy.</p> |
| 6. Enable the SSL client to authenticate servers through digital certificates. | <b>server-verify enable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | By default, SSL server authentication is enabled.                                                                                                     |

## Displaying and maintaining SSL

Execute **display** commands in any view.

| Task                                   | Command                                                 |
|----------------------------------------|---------------------------------------------------------|
| Display SSL server policy information. | <b>display ssl server-policy</b> [ <i>policy-name</i> ] |
| Display SSL client policy information. | <b>display ssl client-policy</b> [ <i>policy-name</i> ] |

## SSL server policy configuration example

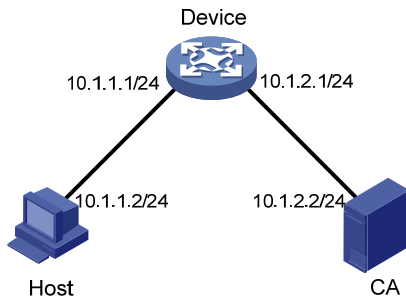
### Network requirements

As shown in [Figure 137](#), users need to access and control the device through the Web page.

To protect the device and prevent data from being eavesdropped or tampered with, configure the device to be accessible to users through HTTPS only.

In this example, the CA server runs Windows Server and has the SCEP plug-in installed.

**Figure 137 Network diagram**



## Configuration considerations

To meet the network requirements, perform the following tasks:

- Configure Device to work as the HTTPS server and request a certificate for Device. For more information about HTTPS, see *Fundamentals Configuration Guide*.
- Request a certificate for Host so that Device can authenticate the identity of Host.

## Configuration procedure

Before performing the following tasks, make sure Device, Host, and the CA server can reach each other.

1. Configure the HTTPS server on Device:

# Create a PKI entity named **en**. Set the common name to **http-server1** and the FQDN to **ssl.security.com** for the entity.

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Create PKI domain **1** and specify the name of the trusted CA as **CA server**. Set the URL of the registration server to **http://10.1.2.2/certsrv/mscep/mscep.dll**, the authority for certificate request to **RA**, and the entity for certificate request to **en**. Set the URL of the CRL repository to **http://10.1.2.2/CertEnroll/caserver.crl**.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier CA server
[Device-pki-domain-1] certificate request url
http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] crl url http://10.1.2.2/CertEnroll/caserver.crl
```

# Configure a general-purpose RSA key pair named **abc** and set the key modulus length to 1024 bits.

```
[Device-pki-domain-1] public-key rsa general name abc length 1024
[Device-pki-domain-1] quit
```

# Generate the RSA key pair named **abc**.

```
[Device] public-key local create rsa name abc
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.....+++++

.....+++++

Create the key pair successfully.

# Obtain the CA certificate.

[Device] pki retrieve-certificate domain 1 ca

The trusted CA's finger print is:

MD5 fingerprint:7682 5865 ACC2 7B16 6F52 D60F D998 4484

SHA1 fingerprint:DF6B C53A E645 5C81 D6FC 09B0 3459 DFD1 94F6 3DDE

Is the finger print correct?(Y/N):y

Retrieved the certificates successfully.

# Generate a certificate request for Device.

[Device] pki request-certificate domain 1

Start to request general certificate ...

Certificate requested successfully.

# Create an SSL server policy named **myssl**.

[Device] ssl server-policy myssl

# Specify PKI domain **1** for the SSL server policy.

[Device-ssl-server-policy-myssl] pki-domain 1

# Enable client authentication.

[Device-ssl-server-policy-myssl] client-verify enable

[Device-ssl-server-policy-myssl] quit

# Configure the HTTPS service to use SSL server policy **myssl**.

[Device] ip https ssl-server-policy myssl

# Enable the HTTPS service.

[Device] ip https enable

# Create a local user named **usera**. Set the password to **123**, service type to **https**, and user role to **network-admin**.

[Device] local-user usera

[Device-luser-usera] password simple 123

[Device-luser-usera] service-type https

[Device-luser-usera] authorization-attribute user-role network-admin

## 2. Request a certificate for Host:

a. Launch IE on Host, and then enter **http://10.1.2.2/certsrv** in the address bar.

b. Request a client certificate for Host. (Details not shown.)

## Verifying the configuration

Perform the following tasks on Host:

1. Launch IE and enter **https://10.1.1.1** in the address bar.

2. Select the certificate issued by the CA server.

The login page of the device should appear.

3. Enter username **usera** and password **123**.

Verify that now you can log in to the Web interface to access and manage the device.

# Configuring ASPF

## Overview

Advanced Stateful Packet Filter (ASPF) is proposed to address the issues that a packet-filter firewall cannot solve. An ASPF provides the following main functions:

- **Application layer protocol inspection**—ASPF checks the application layer information of packets, such as the protocol type and port number, and inspects the application layer protocol status for each connection. ASPF maintains the status information of each connection, and based on the status information, determines whether to permit a packet to pass through the firewall into the internal network. In this way, ASPF defends the internal network against attacks.
- **Transport layer protocol inspection (generic TCP and UDP inspection)**—ASPF checks a TCP/UDP packet's source and destination addresses and port numbers to determine whether to permit the packet to pass through the firewall into the internal network.
- **ICMP error message check**—ASPF inspects the connection information carried in an ICMP error message. If the information does not match the connection, ASPF drops the packet.
- **TCP SYN check**—ASPF checks the first packet of a TCP connection to determine if it is a SYN packet. If it is not a SYN packet, ASPF drops the packet. When a router attached to the network starts up, it can receive a non-SYN packet of an existing TCP connection for the first time. If you do not want to interrupt the existing TCP connection, you can disable the TCP SYN check. The router allows the first non-SYN packet that is used to establish a TCP connection to pass. After the network topology becomes steady, you can enable TCP SYN check again.

At the border of a network, ASPF can work with a packet-filter firewall to provide the network with a more comprehensive security policy that better meets the actual needs. The packet-filter firewall permits or denies packets according to ACL rules. The ASPF records information about the permitted packets to ensure that their return packets can pass through the packet-filter firewall.

## ASPF basic concepts

### Single-channel protocol and multichannel protocol

- **Single-channel protocol**—A single-channel protocol establishes only one connection to exchange both control messages and data for a user. SMTP and HTTP are examples of single-channel protocols.
- **Multichannel protocol**—A multichannel protocol establishes more than one connection for a user and transfers control messages and user data through different connections. FTP is one example of multichannel protocols.

### Internal interface and external interface

On an edge device configured with ASPF to protect hosts and servers on the internal network, the interfaces on the device are divided into internal interfaces and external interface:

- **Internal interfaces**—Interfaces connected to the internal network.
- **External interfaces**—Interfaces connected to the external network.

To protect the internal network, you can apply an ASPF in the outbound direction of the external interfaces or in the inbound direction of the internal interfaces of the device.

### Zone pair

A zone pair specifies the source zone and destination zone of a traffic flow to be inspected:

- **Source zone**—A security zone from which the first packet of a traffic flow originates.

- **Destination zone**—A security zone for which the first packet of a traffic flow is destined.

For information about security zones, see *Fundamentals Configuration Guide*.

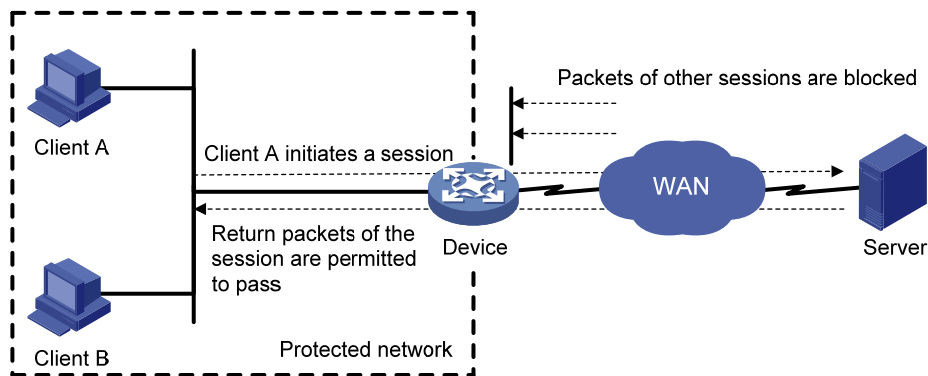
## ASPF inspections

This section introduces the basic idea of ASPF inspection on application layer and transport layer protocols.

### Application layer protocol inspection

As shown in [Figure 138](#), ACLs on the edge device deny incoming packets to the internal network. The ASPF application layer protocol inspection allows return packets from the external network to the internal network.

**Figure 138 Application layer protocol inspection**

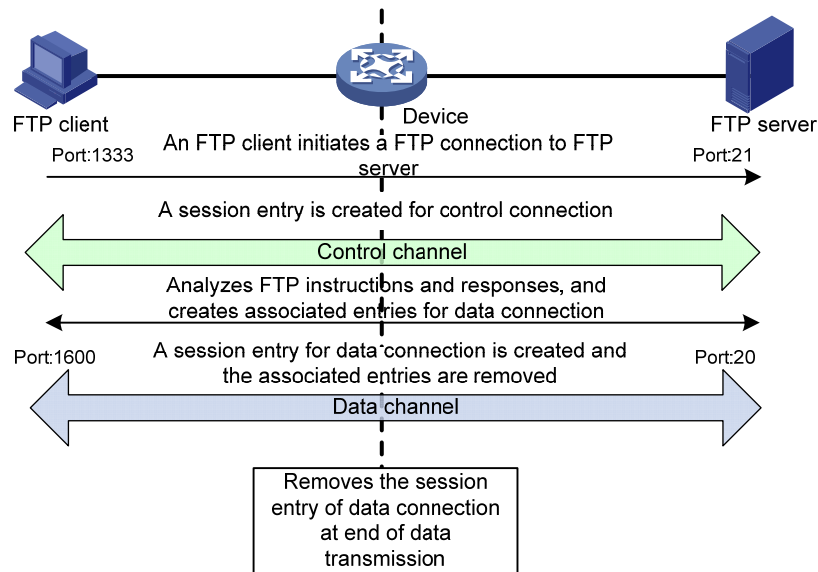


ASPF inspects all application layer sessions as follows:

- For a single-channel protocol, the inspection process is simple.  
ASPF creates a session entry immediately after it detects the session's first packet sent to the external network, and ASPF removes the entry when the connection is terminated.  
The session entry helps record outgoing packets and their return packets. It can maintain the session status and determine whether state transitions of the session are correct. All packets that match a session entry can pass through the packet-filter firewall.
- For a multichannel protocol, ASPF creates session entries, and one or more associated entries to associate the sessions initiated by the same application layer protocol. Associated entries are created during the protocol negotiation and are removed after the negotiation. ASPF uses the associated entries to match the first packets of the sessions. All packets of the sessions matching the associated entries can pass through the packet-filter firewall.

The following uses FTP to explain the process of multichannel application layer protocol inspection.

**Figure 139 FTP inspection**



As shown in Figure 139, FTP connections are established and removed as follows:

1. The FTP client initiates an FTP control connection from port 1333 to port 21 of the FTP server.
2. As a result of negotiation, the server initiates a data connection from port 20 to port 1600 of the client.
3. When data transmission times out or ends, the data connection is removed.

ASPF implements FTP inspection during the FTP connection lifetime as follows:

1. ASPF checks the IP packets the FTP client sends to the FTP server to identify TCP-based FTP packets. Based on the port number, ASPF identifies the control connection between the FTP client and server and creates a control connection session entry.
2. ASPF checks each FTP control connection packet, and examines their TCP status based on the control connection session entry. ASPF analyzes the FTP instructions in the control connection packet. If the packet contains a data channel setup instruction, ASPF creates an associated entry for the data connection.
3. For return FTP control connection packets, ASPF examines their TCP status based on the control connection session entry to make packet forwarding decisions.
4. When the FTP data passes through the device, ASPF is triggered to create a session entry for the data connection and remove the associated entry.
5. For returned FTP data packets, ASPF examines their TCP status based on the data connection session entry to make packet forwarding decisions.
6. When the data transmission ends, ASPF removes the data connection session entry. When the FTP connection is removed, ASPF removes the control connection session entry.

## Transport layer protocol inspection

The transport layer protocol inspection refers to generic TCP/UDP inspection. It creates session entries to record the transport layer information of the packets to dynamically filter TCP and UDP packets. The transport layer information includes source and destination addresses and port numbers.

Generic TCP/UDP inspection requires that return packets must match the corresponding packets that are previously sent out of the external interface. The return packets must have the same source/destination addresses and source/destination port numbers as the outgoing packets (but reversed). Otherwise, the return packets are blocked. For multichannel application layer protocols like FTP, the deployment of TCP inspection without application layer inspection leads to failure of establishing a data connection.

# Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## ASPF configuration task list

| Tasks at a glance                                                                                                                                                                                               | Remarks                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| (Required.) <a href="#">Configuring an ASPF policy</a>                                                                                                                                                          | N/A                                                    |
| (Required.) Applying an ASPF policy: <ul style="list-style-type: none"><li>• <a href="#">Applying an ASPF policy to an interface</a></li><li>• <a href="#">Applying an ASPF policy to a zone pair</a></li></ul> | Perform a task according to your network requirements. |

## Configuring an ASPF policy

Follow these guidelines when you configure an ASPF policy:

- For a multichannel protocol, if you enable TCP or UDP inspection without configuring application layer protocol inspection, the device might not be able to receive return packets. As a best practice, enable application layer protocol inspection together with TCP/UDP inspection.
- For a single-channel protocol, such as Telnet, you only need to configure the transport layer protocol (TCP or UDP) inspection.

To configure an ASPF policy:

| Step                                                                                         | Command                                                                                                                                                                                                                                                                                                                                                                       | Remarks                                                                                             |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                                        | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                            | N/A                                                                                                 |
| 2. Create an ASPF policy and enter its view.                                                 | <b>aspf-policy</b> <i>aspf-policy-number</i>                                                                                                                                                                                                                                                                                                                                  | By default, no ASPF policy exists.                                                                  |
| 3. (Optional.) Configure ASPF inspection for application layer or transport layer protocols. | <b>detect</b> { <i>dccp</i>   <i>dns</i>   <i>ftp</i>   <i>gtp</i>   <i>h323</i>   <i>http</i>   <i>icmp</i>   <i>icmpv6</i>   <i>ils</i>   <i>mgcp</i>   <i>nbt</i>   <i>pptp</i>   <i>rawip</i>   <i>rsh</i>   <i>rtsp</i>   <i>sccp</i>   <i>sctp</i>   <i>sip</i>   <i>smtp</i>   <i>sqlnet</i>   <i>tcp</i>   <i>tftp</i>   <i>udp</i>   <i>udp-lite</i>   <i>xmcp</i> } | By default, ASPF inspection is not configured.                                                      |
| 4. (Optional.) Enable ICMP error message check.                                              | <b>icmp-error drop</b>                                                                                                                                                                                                                                                                                                                                                        | By default, the ICMP error message check is disabled. ASPF does not drop faked ICMP error messages. |



| Step                                 | Command              | Remarks                                                                                                                                 |
|--------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 5. (Optional.) Enable TCP SYN check. | <b>tcp syn-check</b> | By default, TCP SYN check is disabled. ASPF does not drop the non-SYN packet when it is the first packet to establish a TCP connection. |

## Applying an ASPF policy to an interface

You can apply an ASPF policy to inspect incoming or outgoing traffic on an interface. ASPF compares the packets against session entries. If a packet does not match any session entries, ASPF creates a new session entry.

You can apply both ASPF and packet filter to implement packet filtering. For example, you can apply a packet filtering policy to the inbound direction of the external interface and apply an ASPF policy to the outbound direction of the external interface. The application denies unsolicited access from the external network to the internal network and allows return packets from external to the internal network.

Check that a connection initiation packet and the corresponding return packet pass through the same interface, because an ASPF stores and maintains the application layer protocol status based on interfaces.

To apply an ASPF policy on an interface:

| Step                                      | Command                                                                                    | Remarks                                                 |
|-------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------|
| 1. Enter system view.                     | <b>system-view</b>                                                                         | N/A                                                     |
| 2. Enter interface view.                  | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                          | N/A                                                     |
| 3. Apply an ASPF policy to the interface. | <b>aspf apply policy</b><br><i>aspf-policy-number</i> { <b>inbound</b>   <b>outbound</b> } | By default, no ASPF policy is applied to the interface. |

## Applying an ASPF policy to a zone pair

You can apply an ASPF policy to a zone pair to inspect traffic from the source zone to the destination zone. ASPF compares all packets with session entries. If a packet that is permitted by packet filtering does not match any existing session entries, ASPF creates a new session entry.

ASPF for a zone pair takes effect only when it functions with a packet filter:

- The packet filter allows only solicited access from the source zone to the network that the destination zone connects.
- The ASPF policy compares the packets against session entries and allows matching packets from the source zone to the destination zone. The policy also allows return packets from the destination zone to the source zone.

To apply an ASPF policy to a zone pair:

| Step                     | Command                                                                                                        | Remarks                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1. Enter system view.    | <b>system-view</b>                                                                                             | N/A                                                                                        |
| 2. Enter zone pair view. | <b>zone-pair security source</b><br><i>source-zone-name</i> <b>destination</b><br><i>destination-zone-name</i> | For information about configuring a zone pair, see <i>Fundamentals Command Reference</i> . |

| Step                                      | Command                                               | Remarks                                                                                                   |
|-------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| 3. Apply an ASPF policy to the zone pair. | <b>aspf apply policy</b><br><i>aspf-policy-number</i> | By default, the default ASPF policy is applied to the zone pair, which inspects packets of all protocols. |

## Displaying and maintaining ASPF

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                                                                    | Command                                                                                                                         |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Display the configuration of all ASPF policies and their applications to interfaces.                    | <b>display aspf all</b>                                                                                                         |
| Display ASPF policy applications to interfaces.                                                         | <b>display aspf interface</b>                                                                                                   |
| Display the configuration of an ASPF policy.                                                            | <b>display aspf policy</b> <i>aspf-policy-number</i>                                                                            |
| Display ASPF sessions (centralized devices in standalone mode).                                         | <b>display aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ] [ <i>verbose</i> ]                                                    |
| Display ASPF sessions (distributed devices in standalone mode/centralized devices in IRF mode).         | <b>display aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ] [ <i>slot slot-number</i> ] [ <i>verbose</i> ]                        |
| Display ASPF sessions (distributed devices in IRF mode).                                                | <b>display aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ] [ <i>chassis chassis-number slot slot-number</i> ] [ <i>verbose</i> ] |
| Clear ASPF session statistics (centralized devices in standalone mode).                                 | <b>reset aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ]                                                                         |
| Clear ASPF session statistics (distributed devices in standalone mode/centralized devices in IRF mode). | <b>reset aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ] [ <i>slot slot-number</i> ]                                             |
| Clear ASPF session statistics (distributed devices in IRF mode).                                        | <b>reset aspf session</b> [ <i>ipv4</i>   <i>ipv6</i> ] [ <i>chassis chassis-number slot slot-number</i> ]                      |

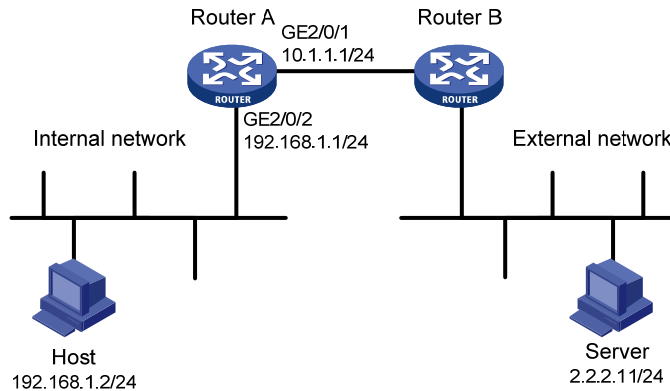
## ASPF configuration examples

### ASPF FTP application inspection configuration example

#### Network requirements

Configure an ASPF policy on Router A to inspect the FTP traffic flows passing through Router A. Only return packets for FTP connections initiated by users on the internal network are permitted to pass through Router A and get into the internal network. All other types of packets from the external network to the internal network are blocked.

**Figure 140 Network diagram**



### Configuration procedure

```
Configure ACL 3111 to deny all IP packets.
<RouterA> system-view
[RouterA] acl advanced 3111
[RouterA-acl-ipv4-adv-3111] rule deny ip
[RouterA-acl-ipv4-adv-3111] quit

Create ASPF policy 1 for FTP inspection.
[RouterA] aspf-policy 1
[RouterA-aspf-policy-1] detect ftp
[RouterA-aspf-policy-1] quit

Apply ACL 3111 to deny all incoming IP packets on interface GigabitEthernet 2/0/1.
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] packet-filter 3111 inbound

Apply ASPF policy 1 to the outbound direction of interface GigabitEthernet 2/0/1..
[RouterA-GigabitEthernet2/0/1] aspf apply policy 1 outbound
```

### Verifying the configuration

# Verify that an ASPF session has been established for the FTP connection between the host and the FTP server.

```
<RouterA> display aspf session ipv4
Initiator:
 Source IP/port: 192.168.1.2/1877
 Destination IP/port: 2.2.2.11/21
 VPN instance/VLAN ID/VLL ID: -/-/-
 Protocol: TCP(6)
```

```
Total sessions found: 1
```

# Verify that only the return packets of FTP connections can enter the internal network. (Details not shown.)

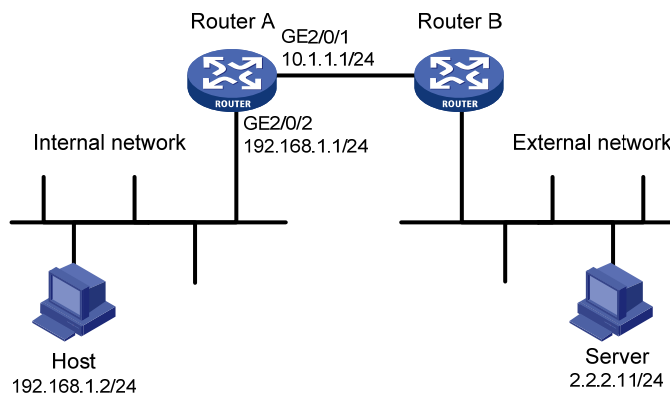
## ASPF TCP application inspection configuration example

### Network requirements

Local users on the internal network need to access the external network. To protect the internal network against ICMP and SYN packet attacks from the external network, configure an ASPF policy

on Router A. Router A can then drop faked ICMP error messages and non-SYN packets that are the first packets over TCP connections.

**Figure 141 Network diagram**



## Configuration procedure

```

Configure ACL 3111 to deny all IP packets.
<RouterA> system-view
[RouterA] acl advanced 3111
[RouterA-acl-ipv4-adv-3111] rule deny ip
[RouterA-acl-ipv4-adv-3111] quit

Create ASPF policy 1.
[RouterA] aspf-policy 1

Enable ICMP error message check.
[RouterA-aspf-policy-1] icmp-error drop

Enable TCP SYN check.
[RouterA-aspf-policy-1] tcp syn-check
[RouterA-aspf-policy-1] quit

Enable ASPF policy 1 to inspect TCP packets.
[RouterA-aspf-policy-1] detect tcp

Apply ACL 3111 to deny all incoming IP packets on interface GigabitEthernet 2/0/1.
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] packet-filter 3111 inbound

Apply ASPF policy 1 to the outbound direction of interface GigabitEthernet 2/0/1.
[RouterA-GigabitEthernet2/0/1] aspf apply policy 1 outbound

```

## Verifying the configuration

```

Display the configuration of ASPF policy 1.
<RouterA> display aspf policy 1
ASPF policy configuration:
 Policy number: 1
 Enable ICMP error message check
 Enable TCP SYN packet check
Detect these protocols:
 TCP

```

Router A can recognize faked ICMP error messages from external networks, and drop the non-SYN packets that are the first packets to establish TCP connections.

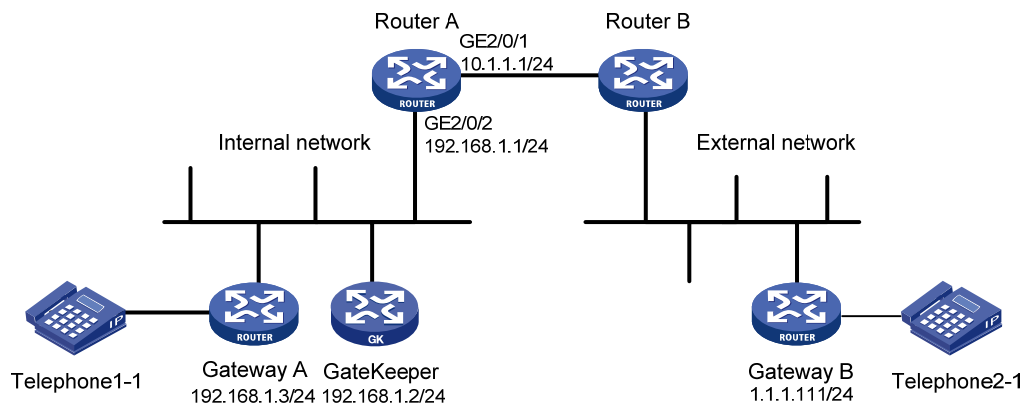
## ASPF H.323 application inspection configuration example

### Network requirements

Figure 142 displays a typical H.323 application network. Gateway B on the external network needs to access the H.323 Gatekeeper, and with the assistance of Gatekeeper, to establish a connection with the H.323 Gateway A. Other protocol packets from the external network are dropped.

Configure a packet filter on Router A to permit only packets destined to the Gatekeeper. Configure an ASPF policy on Router A to detect H.323 protocol packets so that return packets to the external network can be passed through interface GigabitEthernet 2/0/1.

**Figure 142 Network diagram**



### Configuration procedure

# Create ACL 3200 and configure two rules in the ACL: one to permit packets destined to Gatekeeper to pass, and one to deny all IP packets.

```
<RouterA> system-view
[RouterA] acl advanced 3200
[RouterA-acl-ipv4-adv-3200] rule 0 permit ip destination 192.168.1.2 0
[RouterA-acl-ipv4-adv-3200] rule 5 deny ip
[RouterA-acl-ipv4-adv-3200] quit
```

# Create ASPF policy 1 for H.323 inspection.

```
[RouterA] aspf policy 1
[RouterA-aspf-policy-1] detect h323
[RouterA-aspf-policy-1] quit
```

# Apply ACL 3200 to filter incoming packets on interface GigabitEthernet 2/0/1.

```
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] packet-filter 3200 inbound
```

# Apply ASPF policy 1 to the inbound direction of interface GigabitEthernet 2/0/1.

```
[RouterA-GigabitEthernet2/0/1] aspf apply policy 1 inbound
[RouterA-GigabitEthernet2/0/1] quit
```

### Verifying the configuration

# Verify that ASPF sessions have been created between Gateway B and Gatekeeper/Gateway A.

```
[RouterA] display aspf session ipv4
Initiator:
```

Source IP/port: 1.1.1.111/33184  
Destination IP/port: 192.168.1.3/32828  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: UDP(17)

Initiator:

Source IP/port: 1.1.1.111/1719  
Destination IP/port: 192.168.1.2/1719  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: UDP(17)

Initiator:

Source IP/port: 1.1.1.111/3521  
Destination IP/port: 192.168.1.2/20155  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: TCP(6)

Initiator:

Source IP/port: 1.1.1.111/33185  
Destination IP/port: 192.168.1.3/32829  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: UDP(17)

Initiator:

Source IP/port: 1.1.1.111/3688  
Destination IP/port: 192.168.1.2/1720  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: TCP(6)

Total sessions found: 5

# Verify that only return packets that match the entries can pass through GigabitEthernet 2/0/1.  
(Details not shown.)

## ASPF application to a zone pair configuration example

The following matrix shows the configuration example and hardware compatibility:

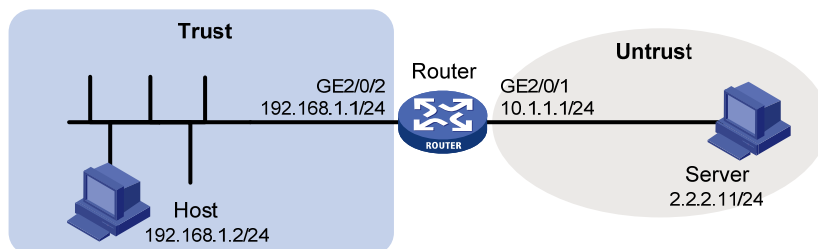
| Hardware                             | Configuration example compatibility |
|--------------------------------------|-------------------------------------|
| MSR954(JH296A/JH297A/ JH298A/JH299A) | No                                  |
| MSR1002-4/1003-8S                    | Yes                                 |
| MSR2003                              | Yes                                 |
| MSR2004-24/2004-48                   | Yes                                 |
| MSR3012/3024/3044/3064               | Yes                                 |
| MSR4060/4080                         | Yes                                 |

## Network requirements

Configure an ASPF policy on Router A to inspect FTP traffic that passes through Router A to implement the following filtering:

- Permits only return packets for the FTP connections initiated by users on the internal network to pass through Router A.
- Blocks all other types of packets from the external network to the internal network.

**Figure 143 Network diagram**



## Configuration procedure

# Configure ACL 3500 to permit IP packets.

```
<Router> system-view
[Router] acl advanced 3500
[Router-acl-ipv4-adv-3500] rule permit ip
[Router-acl-ipv4-adv-3500] quit
```

# Add GigabitEthernet 2/0/2 to security zone **Trust**.

```
[Router] security-zone name trust
[Router-security-zone-Trust] import interface gigabitethernet 2/0/2
[Router-security-zone-Trust] quit
```

# Add GigabitEthernet 2/0/1 to security zone **Untrust**.

```
[Router] security-zone name untrust
[Router-security-zone-Untrust] import interface gigabitethernet 2/0/1
[Router-security-zone-Untrust] quit
```

# Create ASPF policy 1 for FTP inspection.

```
[Router] aspf policy 1
[Router-aspf-policy-1] detect ftp
[Router-aspf-policy-1] quit
```

# Create a zone pair and enter its view.

```
[Router] zone-pair security source trust destination untrust
```

# Apply the ACL to filter to permit outgoing packets in the zone pair.

```
[Router-zone-pair-security-Trust-Untrust] packet-filter 3500
```

# Apply the ASPF policy to the zone pair.

```
[Router-zone-pair-security-Trust-Untrust] aspf apply policy 1
[Router-zone-pair-security-Trust-Untrust] quit
```

## Verifying the configuration

# Verify that an ASPF session has been established for the FTP connection between the host and the server.

```
<Router> display aspf session ipv4
Initiator:
```

Source IP/port: 192.168.1.2/1877  
Destination IP/port: 2.2.2.11/21  
VPN instance/VLAN ID/VLL ID: -/-/-  
Protocol: TCP(6)

Total sessions found: 1

# Verify that only return packets that match the entries can enter the internal network. (Details not shown.)



# Configuring APR

## Overview

The application recognition (APR) feature enables QoS and ASPF to recognize application protocols of packets sent on ports that are not well known. APR separately counts the number of packets or bytes that an interface has received or sent based on application protocols. It also calculates the transmission rates of the interface at the same time.

APR uses the following methods to recognize an application protocol:

- Port-based application recognition (PBAR).
- Group-based application recognition.

## PBAR

PBAR maps a port to an application protocol and recognizes packets of the application protocol according to the port-protocol mapping.

The port-protocol mappings include the following types:

- **Predefined**—An application protocol uses the port defined by the system.
- **User-defined**—An application protocol uses the port defined by the user.

PBAR offers the following mappings to maintain and apply user-defined port configuration:

- **General port mapping**—Maps a user-defined port to an application protocol. All packets destined for that port are regarded as packets of the application protocol. For example, if port 2121 is mapped to FTP, all packets destined for that port are regarded as FTP packets.
- **Host-port mapping**—Maps a user-defined port to an application protocol for packets to or from some specific hosts. For example, you can establish a host-port mapping so that all packets destined for the network segment 10.110.0.0/16 on port 2121 are regarded as FTP packets. To define the range of the hosts, you can specify the ACL, the host IP address range, or the subnet.

Host-port mapping can be further divided into the following categories:

- **ACL-based host-port mapping**—Maps a port to an application protocol for the packets matching the specified ACL.
- **Subnet-based host-port mapping**—Maps a port to an application protocol for the packets sent to the specified subnet.
- **IP address-based host-port mapping**—Maps a port to an application protocol for the packets destined for the specified IP addresses.

## Group-based application recognition

Group-based application recognition adds an application protocol to an application group and obtains the unique properties of the application protocol (for example, the mapped port). APR recognizes packets of the application protocol by matching the packet contents with the unique properties.

You can add application protocols with the same properties to one application group, or copy application protocols from one application group to another.

If a packet is recognized as the packet of an application protocol in an application group, the packet is considered to be the packet of the application group. Features such as QoS and ASPF can handle packets belonging to the same group in bulk.

The following types of application groups are available:

- **Predefined**—The predefined application groups exist on the device by default, and you cannot modify or delete these application groups. To display the predefined application groups, use the **display app-group pre-defined** command.
- **User-defined**—The user-defined application groups are manually created, and you can modify or delete these application groups. To display the user-defined application groups, use the **display app-group user-defined** command.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Configuring PBAR

| Step                         | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.        | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 2. Configure a port mapping. | <ul style="list-style-type: none"> <li>• Configure a general port mapping:<br/><b>port-mapping application</b><br/><i>application-name port port-number</i><br/>[ <b>protocol protocol-name</b> ]</li> <li>• Configure an ACL-based host-port mapping:<br/><b>port-mapping application</b><br/><i>application-name port port-number</i><br/>[ <b>protocol protocol-name</b> ] <b>acl [ ipv6 ]</b><br/><i>acl-number</i></li> <li>• Configure a subnet-based host-port mapping:<br/><b>port-mapping application</b><br/><i>application-name port port-number</i><br/>[ <b>protocol protocol-name</b> ] <b>subnet { ip</b><br/><i>ipv4-address { mask-length   mask }   ipv6</i><br/><i>ipv6-address prefix-length }</i><br/>[ <b>vpn-instance vpn-instance-name</b> ]</li> <li>• Configure an IP address-based host-port mapping:<br/><b>port-mapping application</b><br/><i>application-name port port-number</i><br/>[ <b>protocol protocol-name</b> ] <b>host { ip  </b><br/><b>ipv6 }</b> <i>start-ip-address [ end-ip-address ]</i><br/>[ <b>vpn-instance vpn-instance-name</b> ]</li> </ul> | <p>By default, all application protocols map with well-known ports.</p> <p>You can configure these commands together.</p> <p>APR selects a port mapping to recognize the application protocol of a packet in the following order:</p> <ul style="list-style-type: none"> <li>• IP address-based host-port mapping.</li> <li>• Subnet-based host-port mapping.</li> <li>• ACL-based host-port mapping.</li> <li>• General port mapping.</li> </ul> <p>For the same type of mappings, the mapping with a transport layer protocol has higher priority than the mapping without a transport layer protocol.</p> <p>If the specified application protocol does not exist, the system first creates the protocol.</p> |

# Configuring application groups

The device supports a maximum of 65536 applications groups, and each application group contains a maximum of 65536 user-defined application protocols.

To configure an application group:

| Step                                                                           | Command                                               | Remarks                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                          | <b>system-view</b>                                    | N/A                                                                                                                                                                                                                                                                             |
| 2. Create an application group and enter application group view.               | <b>app-group</b> <i>group-name</i>                    | By default, predefined application groups exist on the device.<br>You cannot modify or delete the predefined application groups.                                                                                                                                                |
| 3. (Optional.) Configure a description for the user-defined application group. | <b>description</b> <i>group-description</i>           | By default, the description is "User-defined application group."                                                                                                                                                                                                                |
| 4. Add an application protocol to the group.                                   | <b>include application</b><br><i>application-name</i> | By default, the user-defined application group does not contain any application protocols.<br>Execute this command multiple times to add multiple application protocols to the group.<br>If the specified application protocol does not exist, the device creates the protocol. |
| 5. Copy all application protocols from another group to the group.             | <b>copy app-group</b> <i>group-name</i>               | Execute this command multiple times to copy application protocols from multiple groups to the current group.                                                                                                                                                                    |

## Enabling application statistics on an interface

### ! IMPORTANT:

The application statistics feature consumes large amount of system memory. When the system generates an alarm for lack of memory, disable the application statistics feature on all interfaces.

If the application statistics feature is enabled on an interface, the device separately counts the number of packets or bytes that the interface has received or sent for each application protocol. It also calculates the transmission rates of the interface for these protocols.

To display application statistics, use the **display application statistics** command.

To enable the application statistics feature on an interface:

| Step                             | Command                                                           | Remarks |
|----------------------------------|-------------------------------------------------------------------|---------|
| 1. Enter system view.            | <b>system-view</b>                                                | N/A     |
| 2. Enter Layer 3 interface view. | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A     |

| Step                                              | Command                                                                      | Remarks                                                                                                                                                  |
|---------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Enable application statistics on an interface. | <b>application statistics enable</b><br>[ <b>inbound</b>   <b>outbound</b> ] | By default, this feature is disabled.<br>You can enable the application statistics feature on both the inbound and outbound directions of the interface. |

## Displaying and maintaining APR

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                                                                                                                                                       | Command                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display information about application protocols.                                                                                                                                           | <b>display application</b> [ <b>name</b> <i>application-name</i>   <b>pre-defined</b>   <b>user-defined</b> ]                                                                                                                                                             |
| Display information about application groups.                                                                                                                                              | <b>display app-group</b> [ <b>name</b> <i>group-name</i>   <b>pre-defined</b>   <b>user-defined</b> ]                                                                                                                                                                     |
| Display statistics for the specified application protocols (centralized devices in standalone mode).                                                                                       | <b>display application statistics</b> [ <b>direction</b> { <b>inbound</b>   <b>outbound</b> }   <b>interface</b> <i>interface-type interface-number</i>   <b>name</b> <i>application-name</i> ] *                                                                         |
| Display statistics for the specified application protocols (distributed devices in standalone mode/centralized devices in IRF mode).                                                       | <b>display application statistics</b> [ <b>direction</b> { <b>inbound</b>   <b>outbound</b> }   <b>interface</b> <i>interface-type interface-number</i> [ <b>slot</b> <i>slot-number</i> ]   <b>name</b> <i>application-name</i> ] *                                      |
| Display statistics for the specified application protocols (distributed devices in IRF mode).                                                                                              | <b>display application statistics</b> [ <b>direction</b> { <b>inbound</b>   <b>outbound</b> }   <b>interface</b> <i>interface-type interface-number</i> [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]   <b>name</b> <i>application-name</i> ] * |
| Display statistics for application protocols on an interface in descending order based on the specified criteria (centralized devices in standalone mode).                                 | <b>display application statistics top number</b> { <b>bps</b>   <b>bytes</b>   <b>packets</b>   <b>pps</b> } <b>interface</b> <i>interface-type interface-number</i>                                                                                                      |
| Display statistics for application protocols on an interface in descending order based on the specified criteria (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display application statistics top number</b> { <b>bps</b>   <b>bytes</b>   <b>packets</b>   <b>pps</b> } <b>interface</b> <i>interface-type interface-number</i> [ <b>slot</b> <i>slot-number</i> ]                                                                   |
| Display statistics for application protocols on an interface in descending order based on the specified criteria (distributed devices in IRF mode).                                        | <b>display application statistics top number</b> { <b>bps</b>   <b>bytes</b>   <b>packets</b>   <b>pps</b> } <b>interface</b> <i>interface-type interface-number</i> [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                              |
| Display information about predefined port mappings.                                                                                                                                        | <b>display port-mapping pre-defined</b>                                                                                                                                                                                                                                   |
| Display information about user-defined port mappings.                                                                                                                                      | <b>display port-mapping user-defined</b> [ <b>application</b> <i>application-name</i>   <b>port</b> <i>port-number</i> ]                                                                                                                                                  |
| Clear application statistics for an interface or all interfaces.                                                                                                                           | <b>reset application statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]                                                                                                                                                                           |

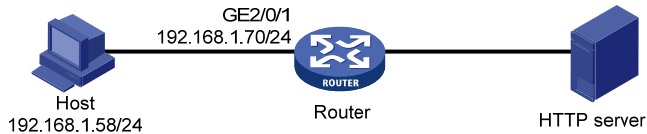
# APR configuration example

## Network requirements

As shown in [Figure 144](#), configure APR on the router to recognize the HTTP packets sent by the host and destined for port 8080.

The router drops the packets recognized by APR.

**Figure 144 Network diagram**



## Configuration procedure

# Create an application group named **group1**, and enter application group view.

```
<Router> system-view
```

```
[Router] app-group group1
```

# Add HTTP to the application group.

```
[Router-app-group-group1] include application http
```

```
[Router-app-group-group1] quit
```

# Map HTTP to TCP and port 8080.

```
[Router] port-mapping application http port 8080 protocol tcp
```

# Create a traffic class named **classifier\_1**, and match **group1** to the class.

```
[Router] traffic classifier classifier_1
```

```
[Router-classifier-classifier_1] if-match app-group group1
```

```
[Router-classifier-classifier_1] quit
```

# Create a traffic behavior named **bdeny**, and configure the action as **deny**.

```
[Router] traffic behavior bdeny
```

```
[Router-behavior-bdeny] filter deny
```

```
[Router-behavior-bdeny] quit
```

# Create QoS policy **1**, associate **classifier\_1** with traffic behavior **bdeny** to create a class-behavior association in the QoS policy.

```
[Router] qos policy 1
```

```
[Router-qospolicy-1] classifier classifier_1 behavior bdeny
```

```
[Router-qospolicy-1] quit
```

# Apply the QoS policy to the inbound direction of interface GigabitEthernet 2/0/1.

```
[Router] interface gigabitethernet 2/0/1
```

```
[Router-GigabitEthernet2/0/1] qos apply policy 1 inbound
```

```
[Router-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

# Verify that the host fails to establish an HTTP connection with the public network. (Details not shown.)

# Managing sessions

## Overview

Session management is a common module, providing basic services for NAT, ASPF, and intrusion detection and protection to implement their session-based services. Session management can be applied for the follow purposes:

- Fast match between packets and sessions.
- Management of transport layer protocol states.
- Identification of application layer protocols.
- Session aging based on protocol states or application layer protocols.
- Persistent sessions.
- Special packet match for the application layer protocols requiring port negotiation.
- ICMP/ICMPv6 error control packet resolution and session match based on the resolution results.

## Session management operation

Session management tracks the session status by inspecting the transport layer protocol information. It updates session states, or ages out sessions according to data flows from the initiators or responders.

When a connection request passes through the device from a client to a server, the device creates a session entry. The entry can contain the request and response information, such as:

- Source IP address and port number.
- Destination IP address and port number.
- Transport layer protocol.
- Application layer protocol.
- Protocol state of the session.

For a multi-channel protocol where the client and the server negotiate a new connection based on an existing connection to implement an application, session management enables the device to create one or more relation entries to associate the connections with the application. A relation entry is created during the negotiation phase and removed after it finishes its support for the multi-channel protocol.

In actual applications, session management works with ASPF to dynamically determine whether a packet can pass the firewall and enter the internal network according to connection status, thus preventing intrusion.

Session management only tracks connection status. It does not block potential attack packets.

## Session management functions

Session management enables the device to provide the following functions:

- Creates sessions for protocol packets, updates session states, and sets aging time for sessions in different protocol states.
- Supports port mapping for application layer protocols (see "Configuring PBAR"), enabling application layer protocols to use customized ports.

- Sets aging time for sessions based on application layer protocols.
- Supports ICMP/ICMPv6 error packet mapping, enabling the device to search for original sessions according to the payloads in the ICMP/ICMPv6 error packets.  
Because error packets are generated due to host errors, the mapping can help speed up the aging of the original sessions.
- Supports persistent sessions, which are kept alive for a long period of time.
- Supports session management for the control channels and dynamic data channels of application layer protocols, for example, FTP.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Session management task list

| Tasks at a glance                                                                                    |
|------------------------------------------------------------------------------------------------------|
| (Optional.) <a href="#">Setting the session aging time for different protocol states</a>             |
| (Optional.) <a href="#">Setting the session aging time for different application layer protocols</a> |
| (Optional.) <a href="#">Specifying persistent sessions</a>                                           |
| (Optional.) <a href="#">Enabling session statistics collection</a>                                   |
| (Optional.) <a href="#">Configuring session logging</a>                                              |

Except for configuring session logging, all other tasks are mutually independent and can be configured in any order.

## Setting the session aging time for different protocol states

### ⚠ IMPORTANT:

If more than 800000 sessions exist, do not set the aging time shorter than the default for a certain protocol state. Short aging time settings can make the device slow in response.

If a session in a certain protocol state has no packet hit before the aging time expires, the device automatically removes the session.

To set the session aging time for different protocol states:

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                                        | Command                                                                                                                                                 | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. Set the session aging time for different protocol states | <b>session aging-time state</b> { fin   icmp-reply   icmp-request   rawip-open   rawip-ready   syn   tcp-est   udp-open   udp-ready } <i>time-value</i> | <p>The default aging time for sessions in different protocol states is as follows:</p> <ul style="list-style-type: none"> <li>• FIN_WAIT: 30 seconds.</li> <li>• ICMP-REPLY: 30 seconds.</li> <li>• ICMP-REQUEST: 60 seconds.</li> <li>• RAWIP-OPEN: 30 seconds.</li> <li>• RAWIP-READY: 60 seconds.</li> <li>• TCP SYN-SENT and SYN-RCV: 30 seconds.</li> <li>• TCP ESTABLISHED: 3600 seconds.</li> <li>• UDP-OPEN: 30 seconds.</li> <li>• UDP-READY: 60 seconds.</li> </ul> |

## Setting the session aging time for different application layer protocols

### ❗ IMPORTANT:

If more than 800000 sessions exist, do not set the aging time shorter than the default for an application layer protocol. Short aging time settings can make the device slow in response.

The aging time for session of different application layer protocols are valid for TCP sessions in ESTABLISHED state or UDP sessions in READY state. If a session has no packet hit before the aging time expires, the device automatically removes the session. For sessions used by other application layer protocols, the aging time for sessions in different protocol states applies.

Set an appropriate aging time to guarantee protocol packet exchange. For example, if the aging time for FTP session is shorter than the interval for sending FTP keepalive messages, an FTP session cannot be maintained.

To set the session aging time for different application layer protocols:

| Step                                                                     | Command                                                                                                                                                                     | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                    | <b>system-view</b>                                                                                                                                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2. Set the session aging time for different application layer protocols. | <b>session aging-time application</b> { dns   ftp   gtp   h225   h245   ils   mgcp   nbt   pptp   ras   rsh   rtsp   sccp   sip   sqlnet   tftp   xdmcp } <i>time-value</i> | <p>By default, the session aging time is as follows:</p> <ul style="list-style-type: none"> <li>• DNS: 60 seconds.</li> <li>• FTP: 3600 seconds.</li> <li>• GTP: 60 seconds.</li> <li>• H.225: 3600 seconds.</li> <li>• H.245: 3600 seconds.</li> <li>• ILS: 3600 seconds.</li> <li>• MGCP: 60 seconds.</li> <li>• NBT: 3600 seconds.</li> <li>• PPTP: 3600 seconds.</li> <li>• RAS: 300 seconds.</li> <li>• RSH: 60 seconds.</li> </ul> |



| Step | Command | Remarks                                                                                                                                                                                                                          |
|------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |         | <ul style="list-style-type: none"> <li>• RTSP: 3600 seconds.</li> <li>• SCCP: 3600 seconds.</li> <li>• SIP: 300 seconds.</li> <li>• SQLNET: 600 seconds.</li> <li>• TFTP: 60 seconds.</li> <li>• XDMCP: 3600 seconds.</li> </ul> |

## Specifying persistent sessions

This task is only for TCP sessions in ESTABLISHED state. You can specify TCP sessions that match the permit statements in the specified ACL as persistent sessions, and set longer lifetime or never-age-out persistent sessions. A never-age-out session is not removed until the device receives a connection close request from the initiator or responder, or you manually clear the session entries.

For a TCP session in ESTABLISHED state, the priority order of the associated aging time is as follows:

- Aging time for persistent sessions.
- Aging time for sessions of application layer protocols.
- Aging time for sessions in different protocol states.

To specify persistent sessions:

| Step                            | Command                                                                         | Remarks                                           |
|---------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------|
| 1. Enter system view.           | <b>system-view</b>                                                              | N/A                                               |
| 2. Specify persistent sessions. | <b>session persistent acl [ ipv6 ]<br/>acl-number [ aging-time time-value ]</b> | By default, no persistent sessions are specified. |

## Enabling session statistics collection

This feature enables the device to collect session-based outbound and inbound packets and bytes.

To display statistics per session, use the **display session table** command. To display statistics per packet type, use the **display session statistics** command.

To enable session statistics collection:

| Step                                     | Command                          | Remarks                                                |
|------------------------------------------|----------------------------------|--------------------------------------------------------|
| 1. Enter system view.                    | <b>system-view</b>               | N/A                                                    |
| 2. Enable session statistics collection. | <b>session statistics enable</b> | By default, session statistics collection is disabled. |

## Configuring session logging

Session logs provide information about user access, IP address translation, and network traffic for security auditing. These logs are sent to the log server or the information center.

The device supports time-based or traffic-based logging:

- **Time-based logging**—The device outputs session logs at an interval.

- **Traffic-based logging**—The device outputs a session log when the traffic amount of a session reaches a threshold. After outputting a session log, the device resets the traffic counter for the session. The traffic-based thresholds can be byte-based and packet-based. If you set both thresholds, the last configuration takes effect.

If you set both time-based and traffic-based logging, the device outputs a session log when whichever is reached. After outputting a session log, the device resets the traffic counter and restarts the interval for the session.

If you enable session logging but specify neither the traffic-based nor the time-based type, the device outputs a session log when a session entry is created or removed.

To configure session logging:

| Step                                             | Command                                                                                                                                                                                                                                    | Remarks                                                                                    |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1. Enter system view.                            | <b>system-view</b>                                                                                                                                                                                                                         | N/A                                                                                        |
| 2. (Optional.) Set a time-based logging type.    | <b>session log time-active</b> <i>time-value</i>                                                                                                                                                                                           | By default, the device does not output session logs.                                       |
| 3. (Optional.) Set a traffic-based logging type. | <ul style="list-style-type: none"> <li>Set the packet-based threshold:<br/><b>session log packets-active</b> <i>packets-value</i></li> <li>Set the byte-based threshold:<br/><b>session log bytes-active</b> <i>bytes-value</i></li> </ul> | The device does not output session logs based on the packet-based or byte-based threshold. |
| 4. Enter interface view.                         | <b>interface</b> <i>interface-type interface-number</i>                                                                                                                                                                                    | N/A                                                                                        |
| 5. Enable session logging.                       | <b>session log enable</b> { <b>ipv4</b>   <b>ipv6</b> } [ <b>acl</b> <i>acl-number</i> ] { <b>inbound</b>   <b>outbound</b> }                                                                                                              | By default, session logging is disabled.                                                   |

## Displaying and maintaining session management

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                                                                         | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display the aging time for sessions of different application layer protocols.                                | <b>display session aging-time application</b>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Display the aging time for sessions in different protocol states.                                            | <b>display session aging-time state</b>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Display IPv4 session table entries (centralized devices in standalone mode).                                 | <b>display session table ipv4</b> [ <b>source-ip</b> <i>start-source-ip</i> [ <i>end-source-ip</i> ] ] [ <b>destination-ip</b> <i>start-destination-ip</i> [ <i>end-destination-ip</i> ] ] [ <b>protocol</b> { <b>dccp</b>   <b>icmp</b>   <b>raw-ip</b>   <b>sctp</b>   <b>tcp</b>   <b>udp</b>   <b>udp-lite</b> } ] [ <b>source-port</b> <i>source-port</i> ] [ <b>destination-port</b> <i>destination-port</i> ] [ <b>verbose</b> ]                                    |
| Display IPv4 session table entries (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display session table ipv4</b> [ <b>slot</b> <i>slot-number</i> ] [ <b>source-ip</b> <i>start-source-ip</i> [ <i>end-source-ip</i> ] ] [ <b>destination-ip</b> <i>start-destination-ip</i> [ <i>end-destination-ip</i> ] ] [ <b>protocol</b> { <b>dccp</b>   <b>icmp</b>   <b>raw-ip</b>   <b>sctp</b>   <b>tcp</b>   <b>udp</b>   <b>udp-lite</b> } ] [ <b>source-port</b> <i>source-port</i> ] [ <b>destination-port</b> <i>destination-port</i> ] [ <b>verbose</b> ] |

| Task                                                                                                         | Command                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display IPv4 session table entries (distributed devices in IRF mode).                                        | <b>display session table ipv4</b> [ chassis chassis-number slot slot-number ] [ source-ip start-source-ip [ end-source-ip ] ] [ destination-ip start-destination-ip [ end-destination-ip ] ] [ protocol { dccp   icmp   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ verbose ]   |
| Display IPv6 session table entries (centralized devices in standalone mode).                                 | <b>display session table ipv6</b> [ source-ip start-source-ip [ end-source-ip ] ] [ destination-ip start-destination-ip [ end-destination-ip ] ] [ protocol { dccp   icmpv6   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ verbose ]                                             |
| Display IPv6 session table entries (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display session table ipv6</b> [ slot slot-number ] [ source-ip start-source-ip [ end-source-ip ] ] [ destination-ip start-destination-ip [ end-destination-ip ] ] [ protocol { dccp   icmpv6   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ verbose ]                        |
| Display IPv6 session table entries (distributed devices in IRF mode).                                        | <b>display session table ipv6</b> [ chassis chassis-number slot slot-number ] [ source-ip start-source-ip [ end-source-ip ] ] [ destination-ip start-destination-ip [ end-destination-ip ] ] [ protocol { dccp   icmpv6   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ verbose ] |
| Display session statistics (centralized devices in standalone mode).                                         | <b>display session statistics</b> [ summary ]                                                                                                                                                                                                                                                                                                    |
| Display session statistics (distributed devices in standalone mode/centralized devices in IRF mode).         | <b>display session statistics</b> [ summary ] [ slot slot-number ]                                                                                                                                                                                                                                                                               |
| Display session statistics (distributed devices in IRF mode).                                                | <b>display session statistics</b> [ summary ] [ chassis chassis-number slot slot-number ]                                                                                                                                                                                                                                                        |
| Display relation table entries (centralized devices in standalone mode).                                     | <b>display session relation-table</b> { ipv4   ipv6 }                                                                                                                                                                                                                                                                                            |
| Display relation table entries (distributed devices in standalone mode/centralized devices in IRF mode).     | <b>display session relation-table</b> { ipv4   ipv6 } [ slot slot-number ]                                                                                                                                                                                                                                                                       |
| Display relation table entries (distributed devices in IRF mode).                                            | <b>display session relation-table</b> { ipv4   ipv6 } [ chassis chassis-number slot slot-number ]                                                                                                                                                                                                                                                |
| Clear IPv4 session table entries (centralized devices in standalone mode).                                   | <b>reset session table ipv4</b> [ source-ip source-ip ] [ destination-ip destination-ip ] [ protocol { dccp   icmp   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ vpn-instance vpn-instance-name ]                                                                               |
| Clear IPv4 session table entries (distributed devices in standalone mode/centralized devices in IRF mode).   | <b>reset session table ipv4</b> [ slot slot-number ] [ source-ip source-ip ] [ destination-ip destination-ip ] [ protocol { dccp   icmp   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ vpn-instance vpn-instance-name ]                                                          |
| Clear IPv4 session table entries (distributed devices in IRF mode).                                          | <b>reset session table ipv4</b> [ chassis chassis-number slot slot-number ] [ source-ip source-ip ] [ destination-ip destination-ip ] [ protocol { dccp   icmp   raw-ip   sctp   tcp   udp   udp-lite } ] [ source-port source-port ] [ destination-port destination-port ] [ vpn-instance vpn-instance-name ]                                   |

| Task                                                                                                                | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clear IPv6 session table entries (centralized devices in standalone mode).                                          | <b>reset session table ipv6</b> [ <b>source-ip</b> <i>source-ip</i> ] [ <b>destination-ip</b> <i>destination-ip</i> ] [ <b>protocol</b> { <b>dccp</b>   <b>icmpv6</b>   <b>raw-ip</b>   <b>sctp</b>   <b>tcp</b>   <b>udp</b>   <b>udp-lite</b> } ] [ <b>source-port</b> <i>source-port</i> ] [ <b>destination-port</b> <i>destination-port</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]                                                                         |
| Clear IPv6 session table entries (distributed devices in standalone mode/centralized devices in IRF mode).          | <b>reset session table ipv6</b> [ <b>slot</b> <i>slot-number</i> ] [ <b>source-ip</b> <i>source-ip</i> ] [ <b>destination-ip</b> <i>destination-ip</i> ] [ <b>protocol</b> { <b>dccp</b>   <b>icmpv6</b>   <b>raw-ip</b>   <b>sctp</b>   <b>tcp</b>   <b>udp</b>   <b>udp-lite</b> } ] [ <b>source-port</b> <i>source-port</i> ] [ <b>destination-port</b> <i>destination-port</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]                                      |
| Clear IPv6 session table entries (distributed devices in IRF mode).                                                 | <b>reset session table ipv6</b> [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>source-ip</b> <i>source-ip</i> ] [ <b>destination-ip</b> <i>destination-ip</i> ] [ <b>protocol</b> { <b>dccp</b>   <b>icmpv6</b>   <b>raw-ip</b>   <b>sctp</b>   <b>tcp</b>   <b>udp</b>   <b>udp-lite</b> } ] [ <b>source-port</b> <i>source-port</i> ] [ <b>destination-port</b> <i>destination-port</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] |
| Clear IPv4 and IPv6 session table entries (centralized devices in standalone mode).                                 | <b>reset session table</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Clear IPv4 and IPv6 session table entries (distributed devices in standalone mode/centralized devices in IRF mode). | <b>reset session table</b> [ <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                              |
| Clear IPv4 and IPv6 session table entries (distributed devices in IRF mode).                                        | <b>reset session table</b> [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                         |
| Clear session statistics (centralized devices in standalone mode).                                                  | <b>reset session statistics</b>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Clear session statistics (distributed devices in standalone mode/centralized devices in IRF mode).                  | <b>reset session statistics</b> [ <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                         |
| Clear session statistics (distributed devices in IRF mode).                                                         | <b>reset session statistics</b> [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                    |
| Clear relation table entries (centralized devices in standalone mode).                                              | <b>reset session relation-table</b> [ <b>ipv4</b>   <b>ipv6</b> ]                                                                                                                                                                                                                                                                                                                                                                                                          |
| Clear relation table entries (distributed devices in standalone mode/centralized devices in IRF mode).              | <b>reset session relation-table</b> [ <b>ipv4</b>   <b>ipv6</b> ] [ <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                       |
| Clear relation table entries (distributed devices in IRF mode).                                                     | <b>reset session relation-table</b> [ <b>ipv4</b>   <b>ipv6</b> ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                  |

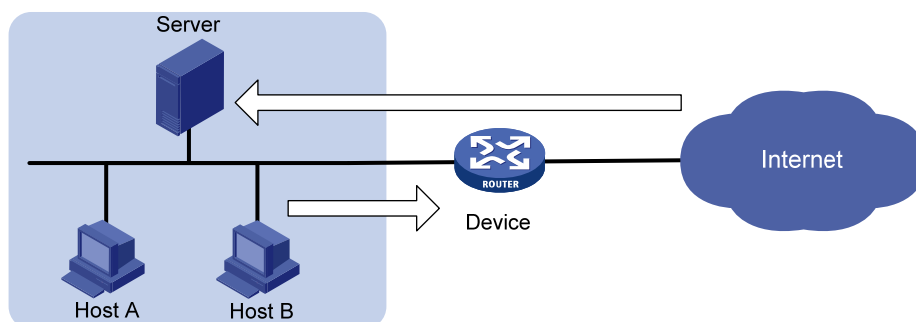
# Configuring connection limits

The connection limit feature enables the device to monitor and limit the number of established connections.

As shown in [Figure 145](#), the following problems might exist:

- If Host B initiates a large number of connections in a short period of time, it might exhaust system resources and cause Host A to be unable to access the Internet.
- If the internal server receives a large number of connection requests in a short period of time, the server cannot process other requests.

**Figure 145 Network diagram**



To resolve these problems, configure connection limits on the interfaces of the device.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Interface-based connection limit configuration task list

| Tasks at a glance                                                   |
|---------------------------------------------------------------------|
| (Required.) <a href="#">Creating a connection limit policy</a>      |
| (Required.) <a href="#">Configuring the connection limit policy</a> |
| (Required.) <a href="#">Applying the connection limit policy</a>    |

# Creating a connection limit policy

A connection limit policy contains a set of connection limit rules, each of which defines a range of connections and the criteria for limiting the connections.

To create a connection limit policy:

| Step                                                    | Command                                                    | Remarks                                         |
|---------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------|
| 1. Enter system view.                                   | <b>system-view</b>                                         | N/A                                             |
| 2. Create a connection limit policy and enter its view. | <b>connection-limit { ipv6-policy   policy } policy-id</b> | By default, no connection limit policies exist. |

## Configuring the connection limit policy

To use a connection limit policy, you need to add limit rules to the policy. Each rule defines a range of connections and the criteria for limiting the connections. Connections in the range will be limited based on the criteria. When the number of matching connections reaches the upper limit, the device does not accept new connections until the number of connections drops below the lower limit. The connections that do not match any connection limit rules are not limited.

In each connection limit rule, an ACL is referenced to define the connection range. In addition, the rule also uses the following filtering methods to further limit the connections:

- **per-destination**—Limits user connections by destination IP address.
- **per-service**—Limits user connections by service (transport layer protocol and service port).
- **per-source**—Limits user connections by source IP address.
- **per-ds-lite-b4**— Limits user connections by the B4 device on a DS-Lite tunnel. For information about DS-Lite tunnels, see *Layer 3 IP Services Configuration Guide*.

You can select more than one filtering method, and the selected methods take effect at the same time. For example, if you specify both **per-destination** and **per-service**, the user connections using the same service and destined to the same IP address are limited. If you do not specify any filtering methods in a limit rule, all user connections in the range are limited.

When a connection limit policy is applied, connections on the device match all limit rules in the policy in ascending order of rule IDs. As a best practice, specify a smaller range and more filtering methods in a rule with a smaller ID.

To configure the connection limit policy:

| Step                                   | Command                                                                                                                                                                                                                                                                                                                                                          | Remarks                                      |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| 1. Enter system view.                  | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                               | N/A                                          |
| 2. Enter connection limit policy view. | <b>connection-limit { ipv6-policy   policy } policy-id</b>                                                                                                                                                                                                                                                                                                       | N/A                                          |
| 3. Configure a connection limit rule.  | <ul style="list-style-type: none"><li>• IPv4 connection limit policy view:<br/><b>limit limit-id acl [ ipv6 ] { acl-number   name acl-name } [ per-destination   per-service   per-source ] * amount max-amount min-amount</b><br/>IPv6 connection limit policy view:<br/><b>limit limit-id acl ipv6 { acl-number   name acl-name } per-ds-lite-b4</b></li></ul> | By default, no connection limit rules exist. |

| Step | Command                                                                                                                                                                                                                                                                                                                                                                                           | Remarks |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|      | <b>amount</b> <i>max-amount</i><br><i>min-amount</i> <ul style="list-style-type: none"> <li>IPv6 connection limit policy view:<br/> <b>limit</b> <i>limit-id</i> <b>acl ipv6</b><br/> { <i>acl-number</i>   <b>name</b><br/> <i>acl-name</i> } [ <b>per-destination</b><br/>   <b>per-service</b>   <b>per-source</b> ]<br/> * <b>amount</b> <i>max-amount</i><br/> <i>min-amount</i> </li> </ul> |         |

## Applying the connection limit policy

To make a connection limit policy take effect, apply it globally or to an interface. The connection limit policy applied to an interface takes effect only on the specified connections on the interface. The connection limit policy applied globally takes effect on all the specified connections on the device.

Different connection limit policies can be applied to individual interfaces as well as globally on the device. In this case, the device matches connections against these policies in the order of the policy on the inbound interface, the global policy, and the policy on the outbound interface. It cannot accept new connections as long as the number of connections reaches the lowest upper connection limit defined by these policies.

On a DS-Lite tunnel network, if the AFTR device uses the Endpoint-Independent Mapping-based NAT configuration, you must limit connections from external IPv4 networks to access the internal IPv4 network. To implement B4 device-based connection limits, perform the following tasks:

- Add a rule that has the **per-ds-lite-b4** to a connection limit policy.
- Apply the policy globally or on the DS-Lite tunnel interface.

To apply a connection limit policy:

| Step                                | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Remarks                                                                                                                                                                                                                 |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.               | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                           | N/A                                                                                                                                                                                                                     |
| 2. Apply a connection limit policy. | <ul style="list-style-type: none"> <li>Apply a connection limit policy globally<br/> <b>connection-limit apply global</b> { <b>ipv6-policy</b>   <b>policy</b> } <i>policy-id</i></li> <li>Apply a connection limit policy to an interface. <ul style="list-style-type: none"> <li><b>interface</b> <i>interface-type</i><br/> <i>interface-number</i></li> <li><b>connection-limit apply</b> { <b>ipv6-policy</b>   <b>policy</b> } <i>policy-id</i></li> </ul> </li> </ul> | <p>By default, no connection limit is applied.</p> <p>Only one IPv4 connection limit policy and one IPv6 connection limit policy can be applied. A new IPv4 or IPv6 connection limit policy overwrites the old one.</p> |

## Displaying and maintaining connection limits

Execute **display** commands in any view and **reset** commands in user view.

| Task                                | Command                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------|
| Display the connection limit policy | <b>display connection-limit</b> { <b>ipv6-policy</b>   <b>policy</b> } { <b>all</b>   <i>policy-id</i> } |



| Task                                                                                                                                                                            | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| information.                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Display the connection limit statistics globally or on an interface (centralized devices in standalone mode).                                                                   | <b>display connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Display the connection limit statistics globally or on an interface (distributed devices in standalone mode/centralized devices in IRF mode).                                   | <b>display connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Display the connection limit statistics globally or on an interface (distributed devices in IRF mode).                                                                          | <b>display connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Display statistics about IPv6 connections matching connection limit rules globally or on an interface (centralized devices in standalone mode).                                 | <b>display connection-limit</b> { <b>ipv6-stat-nodes</b>   <b>stat-nodes</b> } { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>destination</b> <i>destination-ip</i>   <b>service-port</b> <i>port-number</i>   <b>source</b> <i>source-ip</i> ] * [ <b>count</b> ]<br><b>display connection-limit stat-nodes</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } <b>dslite-peer</b> <i>b4-address</i> [ <b>count</b> ]                                                                                                                                                 |
| Display statistics about IPv6 connections matching connection limit rules globally or on an interface (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display connection-limit</b> { <b>ipv6-stat-nodes</b>   <b>stat-nodes</b> } { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>slot</b> <i>slot-number</i> ] [ <b>destination</b> <i>destination-ip</i>   <b>service-port</b> <i>port-number</i>   <b>source</b> <i>source-ip</i> ] * [ <b>count</b> ]<br><b>display connection-limit stat-nodes</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>slot</b> <i>slot-number</i> ] <b>dslite-peer</b> <i>b4-address</i> [ <b>count</b> ]                                                                           |
| Display statistics about IPv6 connections matching connection limit rules globally or on an interface (distributed devices in IRF mode).                                        | <b>display connection-limit</b> { <b>ipv6-stat-nodes</b>   <b>stat-nodes</b> } { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>destination</b> <i>destination-ip</i>   <b>service-port</b> <i>port-number</i>   <b>source</b> <i>source-ip</i> ] * [ <b>count</b> ]<br><b>display connection-limit stat-nodes</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] <b>dslite-peer</b> <i>b4-address</i> [ <b>count</b> ] |
| Clear the connection limit statistics globally or on an interface (centralized devices in standalone mode).                                                                     | <b>reset connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Clear the connection limit statistics globally or on an interface (distributed devices in standalone mode/centralized devices in IRF mode).                                     | <b>reset connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Clear the connection limit statistics globally or on an interface (distributed devices in IRF mode).                                                                            | <b>reset connection-limit statistics</b> { <b>global</b>   <b>interface</b> <i>interface-type interface-number</i> } [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Connection limit configuration example

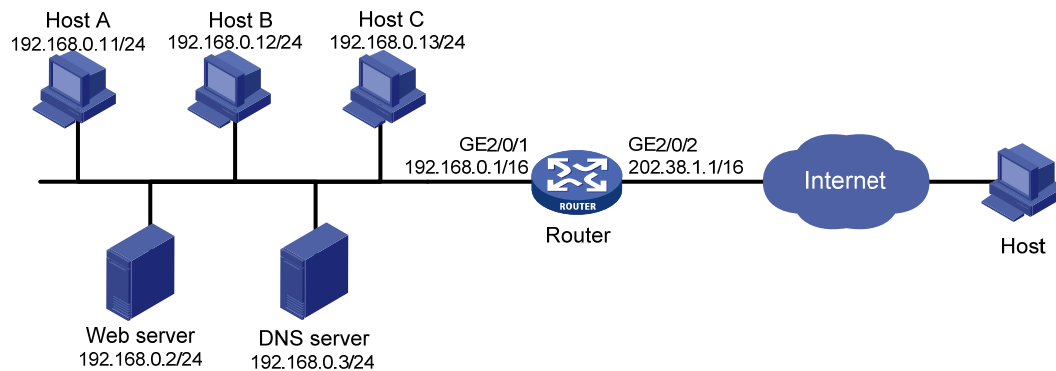
### Network requirements

As shown in [Figure 146](#), a company has five public IP addresses: 202.38.1.1/24 to 202.38.1.5/24. The internal network address is 192.168.0.0/16. Configure NAT so that the internal users can access the Internet and external users can access the internal servers. Configure connection limits to meet the following requirements:



- All hosts on segment 192.168.0.0/24 can establish a maximum of 100000 connections to the external network.
- Each host on segment 192.168.0.0/24 can establish a maximum of 100 connections to the external network.
- A maximum of 10000 query requests from DNS clients to the DNS server are allowed at the same time.
- A maximum of 10000 connection requests from Web clients to the Web server are allowed at the same time.

**Figure 146 Network diagram**



## Configuration procedure

The following example only describes how to configure connection limits. For information about NAT configuration and internal server configuration, see *Layer 3—IP Services Configuration Guide*.

# Create ACL 3000 to permit packets from all hosts on the internal network.

```
<Router> system-view
[Router] acl advanced 3000
[Router-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Router-acl-ipv4-adv-3000] quit
```

# Create ACL 3001 to permit packets to the Web server and the DNS server.

```
[Router] acl advanced 3001
[Router-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[Router-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.3 0
[Router-acl-ipv4-adv-3001] quit
```

# Create connection limit policy 1.

```
[Router] connection-limit policy 1
```

# Configure connection limit rule 1 to permit a maximum of 100000 connections from all the hosts that match ACL 3000. When the number of connections exceeds 100000, new connections cannot be established until the number drops below 95000.

```
[Router-connection-limit-policy-1] limit 1 acl 3000 amount 100000 95000
```

# Configure connection limit rule 2 to permit a maximum of 10000 connections to the servers that match ACL 3001. When the number of connections exceeds 10000, new connections cannot be established until the number drops below 9800.

```
[Router-connection-limit-policy-1] limit 2 acl 3001 per-destination amount 10000 9800
[Router-connection-limit-policy-1] quit
```

# Create connection limit policy 2.

```
[Router] connection-limit policy 2

Configure connection limit rule 1 to permit a maximum of 100 connections from each host matching
ACL 3000. When the number of connections exceeds 100, new connections cannot be established
until the number drops below 90.
[Router-connection-limit-policy-2] limit 1 acl 3000 per-source amount 100 90
[Router-connection-limit-policy-2] quit

Apply connection limit policy 1 globally.
[Router] connection-limit apply global policy 1

Apply connection limit policy 2 to inbound interface GigabitEthernet 2/0/1.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] connection-limit apply policy 2
[Router-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

```
Display information about the connection limit policy.
[Router] display connection-limit policy 1
IPv4 connection limit policy 1 has been applied 1 times, and has 2 limit rules.
Limit rule list:
 Policy Rule StatType HiThres LoThres ACL

 1 1 -- 100000 95000 3000
 1 2 Dst 10000 9800 3001

Applied list:
 Global
[Router] display connection-limit policy 2
IPv4 connection limit policy 2 has been applied 1 times, and has 1 limit rules.
Limit rule list:
 Policy Rule StatType HiThres LoThres ACL

 2 1 Src 100 90 3000

Applied list:
 GigabitEthernet2/0/1
```

## Troubleshooting connection limits

### ACLs in the connection limit rules with overlapping segments

#### Symptom

A connection limit policy has two rules. Rule 1 sets the upper limit to 10 for the connections from each host on segment 192.168.0.0/24. Rule 2 sets the upper limit to 100 for the connections from 192.168.0.100/24.

```
<Router> system-view
[Router] acl basic 2001
[Router-acl-ipv4-basic-2001] rule permit source 192.168.0.0 0.0.0.255
```

```
[Router-acl-ipv4-basic-2001] quit
[Router] acl basic 2002
[Router-acl-ipv4-basic-2002] rule permit source 192.168.0.100 0
[Router-acl-ipv4-basic-2002] quit
[Router] connection-limit policy 1
[Router-connection-limit-policy-1] limit 1 acl 2001 per-destination amount 10 5
[Router-connection-limit-policy-1] limit 2 acl 2002 per-destination amount 100 10
```

As a result, the host at 192.168.0.100 can only initiate a maximum of 10 connections to the external network.

## Analysis

Both limit rules **1** and **2** contain IP address 192.168.0.100. Limit rule 1 is first matched and takes effect to limit the connections from 192.168.0.100.

## Solution

To resolve the problem:

1. Rearrange the two connection limit rules by exchanging their rule IDs.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

# Configuring object groups

## Overview

An object group is a group of objects that can be used by an object policy or object group to identify packets. Object groups are divided into the following types:

- **IPv4 address object group**—A group of IPv4 address objects used to match the IPv4 address in a packet.
- **IPv6 address object group**—A group of IPv6 address objects used to match the IPv6 address in a packet.
- **Port object group**—A group of port objects used to match the protocol port number in a packet.
- **Service object group**—A group of service objects used to match the upper-layer service in a packet.

## Configuring an IPv4 address object group

| Step                                                                      | Command                                                                                                                                                                                                                                                                                     | Remarks                                                      |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 1. Enter system view.                                                     | <b>system-view</b>                                                                                                                                                                                                                                                                          | N/A                                                          |
| 2. Configure an IPv4 address object group and enter its view.             | <b>object-group ip address</b><br><i>object-group-name</i>                                                                                                                                                                                                                                  | The system has one default IPv4 address object group.        |
| 3. (Optional.) Configure a description for the IPv4 address object group. | <b>description</b> <i>text</i>                                                                                                                                                                                                                                                              | By default, an object group does not have a description.     |
| 4. Configure an IPv4 address object.                                      | [ <i>object-id</i> ] <b>network</b> { <b>host</b> { <b>address</b> <i>ip-address</i>   <b>name</b> <i>host-name</i> }   <b>subnet</b> <i>ip-address</i> { <i>mask-length</i>   <b>mask</b> }   <b>range</b> <i>ip-address1 ip-address2</i>   <b>group-object</b> <i>object-group-name</i> } | By default, no object exists in a user-defined object group. |

## Configuring an IPv6 address object group

| Step                                                                      | Command                                                                                                                                                                                  | Remarks                                                      |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 1. Enter system view.                                                     | <b>system-view</b>                                                                                                                                                                       | N/A                                                          |
| 2. Configure an IPv6 address object group and enter its view.             | <b>object-group ipv6 address</b><br><i>object-group-name</i>                                                                                                                             | The system has one default IPv6 address object group.        |
| 3. (Optional.) Configure a description for the IPv6 address object group. | <b>description</b> <i>text</i>                                                                                                                                                           | By default, an object group does not have a description.     |
| 4. Configure an IPv6 address object.                                      | [ <i>object-id</i> ] <b>network</b> { <b>host</b> { <b>address</b> <i>ipv6-address</i>   <b>name</b> <i>host-name</i> }   <b>subnet</b> <i>ipv6-address prefix-length</i>   <b>range</b> | By default, no object exists in a user-defined object group. |

| Step | Command                                                                             | Remarks |
|------|-------------------------------------------------------------------------------------|---------|
|      | <code>ipv6-address1 ipv6-address2  <br/>group-object<br/>object-group-name }</code> |         |

## Configuring a port object group

| Step                                                              | Command                                                                                                                    | Remarks                                                      |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 1. Enter system view.                                             | <b>system-view</b>                                                                                                         | N/A                                                          |
| 2. Configure a port object group and enter its view.              | <b>object-group port</b><br><i>object-group-name</i>                                                                       | The system has one default port object group.                |
| 3. (Optional.) Configure a description for the port object group. | <b>description</b> <i>text</i>                                                                                             | By default, an object group does not have a description.     |
| 4. Configure a port object.                                       | <code>[ object-id ] port { { eq   lt   gt } port<br/>  range port1 port2  <br/>group-object<br/>object-group-name }</code> | By default, no object exists in a user-defined object group. |

## Configuring a service object group

| Step                                                                 | Command                                                                                                                                                                                                                                                                             | Remarks                                                      |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                                                                                                                                                                                                  | N/A                                                          |
| 2. Configure a service object group and enter its view.              | <b>object-group service</b><br><i>object-group-name</i>                                                                                                                                                                                                                             | The system has one default service object group.             |
| 3. (Optional.) Configure a description for the service object group. | <b>description</b> <i>text</i>                                                                                                                                                                                                                                                      | By default, an object group does not have a description.     |
| 4. Configure a service object.                                       | <code>[ object-id ] service { protocol<br/>[ { source { { eq   lt   gt } port   range<br/>port1 port2 }   destination { { eq   lt  <br/>gt } port   range port1 port2 } } *  <br/>icmp-type icmp-code   icmpv6-type<br/>icmpv6-code ]   group-object<br/>object-group-name }</code> | By default, no object exists in a user-defined object group. |

## Displaying and maintaining object groups

Execute **display** commands in any view.

| Task                                     | Command                                                                                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display information about object groups. | <code>display object-group [ { { ip   ipv6 } address   service  <br/>port } [ default ] [ name object-group-name ]   name<br/>object-group-name ]</code> |

# Configuring object policies

## Overview

An object policy is a set of rules for security control over packets between a source and a destination security zone. These two zones define a zone pair. The object policy matches the first packet of a traffic flow against the rules. If a match is found, the device stops the match process and takes the action defined in the rule over the packet and all subsequent packets of the flow.

For more information about zone pair and security zone configuration, see *Fundamentals Configuration Guide*.

## Object policy rules

An object policy contains one or multiple rules. Each object policy rule is a permit or deny statement for identifying traffic based on criteria such as the source IP address, destination IP address, and service type. The identified packets are processed based on actions stated in the rules.

## Rule numbering

Each rule is uniquely identified by an ID. The rule ID can be manually configured or automatically assigned by the system when you create the rule. In automatic rule numbering, the system assigns the rule an integer next to the greatest ID being used. For example, if the greatest ID is 60000, the system automatically assigns 60001. If the greatest ID is 65534, the system assigns the smallest unused rule ID to the rule.

## Rule match order

The system matches packets against rules in the order the rules were configured. The match process stops when a match is found. You can use the **display this** command in zone pair view to check the rule configuration order. You can use the **move rule** command in object policy view to change the rule configuration order.

## Rule description

You can configure a description for each rule to identify different rules in an object policy.

## Object policy configuration task list

| Tasks at a glance                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Required.) <a href="#">Creating object policies</a> :                                                                                                                    |
| <ul style="list-style-type: none"><li>• <a href="#">Creating an IPv4 object policy</a></li><li>• <a href="#">Creating an IPv6 object policy</a></li></ul>                 |
| (Required.) <a href="#">Configuring object policy rules</a> :                                                                                                             |
| <ul style="list-style-type: none"><li>• <a href="#">Configuring an IPv4 object policy rule</a></li><li>• <a href="#">Configuring an IPv6 object policy rule</a></li></ul> |
| (Required.) <a href="#">Applying object policies to zone pairs</a>                                                                                                        |

|                                                                 |
|-----------------------------------------------------------------|
| Tasks at a glance                                               |
| (Optional.) <a href="#">Changing the rule match order</a>       |
| (Optional.) <a href="#">Enabling rule matching acceleration</a> |

## Configuration prerequisites

Before configuring an object policy, complete the following tasks:

- Configure time ranges (see *ACL and QoS Configuration Guide*).
- Configure IPv4 address objects, IPv6 address objects, and service objects (see "[Configuring object groups](#)").

## Creating object policies

### Creating an IPv4 object policy

| Step                                                          | Command                                           | Remarks                                                   |
|---------------------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                                | N/A                                                       |
| 2. Create an IPv4 object policy and enter its view.           | <b>object-policy ip</b> <i>object-policy-name</i> | By default, no object policy exists.                      |
| 3. (Optional.) Configure a description for the object policy. | <b>description</b> <i>text</i>                    | By default, an object policy does not have a description. |

### Creating an IPv6 object policy

| Step                                                          | Command                                             | Remarks                                                   |
|---------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------|
| 1. Enter system view.                                         | <b>system-view</b>                                  | N/A                                                       |
| 2. Create an IPv6 object policy and enter its view.           | <b>object-policy ipv6</b> <i>object-policy-name</i> | By default, no object policy exists.                      |
| 3. (Optional.) Configure a description for the object policy. | <b>description</b> <i>text</i>                      | By default, an object policy does not have a description. |

## Configuring object policy rules

### Configuring an IPv4 object policy rule

You can specify an existing object group in an IPv4 object policy rule for matching target IPv4 packets. If no object group is specified for a rule, the rule applies to all IPv4 packets.

The following object groups can be referenced in a rule for packet matching:

- **Source IPv4 address object group**—Used for matching the source IPv4 addresses of packets.

- **Destination IPv4 address object group**—Used for matching the destination IPv4 addresses of packets.
- **Service object group**—Used for matching the service types carried in packets.
- **VRF instance**—Used for matching the MPLS L3VPN instances of packets.

For more information about object groups, see "[Configuring object groups](#)."

To configure an IPv4 object policy rule:

| Step                                                 | Command                                                                                                                                                                                                                                                                                                                                                                                                  | Remarks                                                                                                                      |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                       | N/A                                                                                                                          |
| 2. Enter IPv4 object policy view.                    | <b>object-policy ip</b> <i>object-policy-name</i>                                                                                                                                                                                                                                                                                                                                                        | N/A                                                                                                                          |
| 3. Configure an IPv4 object policy rule.             | <b>rule</b> [ <i>rule-id</i> ] { <b>drop</b>   <b>pass</b> } [ [ <b>source-ip</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>destination-ip</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>service</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>counting</b> ] [ <b>disable</b> ] [ <b>logging</b> ] [ <b>time-range</b> <i>time-range-name</i> ] ] * | By default, no object policy rule exists.<br><br>If you specify a nonexistent object group, the rule does not match packets. |
| 4. (Optional.) Configure a description for the rule. | <b>rule</b> <i>rule-id</i> <b>comment</b> <i>text</i>                                                                                                                                                                                                                                                                                                                                                    | By default, an object policy rule does not have a description.                                                               |

## Configuring an IPv6 object policy rule

You can specify an existing object group in an IPv6 object policy rule for matching target IPv6 packets. If no object group is specified for a rule, the rule applies to all IPv6 packets.

The following object groups can be referenced in a rule for packet matching:

- **Source IPv6 address object group**—Used for matching the source IPv6 addresses of packets.
- **Destination IPv6 address object group**—Used for matching the destination IPv6 addresses of packets.
- **Service object group**—Used for matching the service types carried in packets.
- **VRF instance**—Used for matching the MPLS L3VPN instances of packets.

For more information about the object groups, see "[Configuring object groups](#)."

To configure an IPv6 object policy rule:

| Step                                     | Command                                                                                                                                                                                                                                                                                                                                                                                                  | Remarks                                                                                                                      |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                    | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                       | N/A                                                                                                                          |
| 2. Enter IPv6 object policy view.        | <b>object-policy ipv6</b> <i>object-policy-name</i>                                                                                                                                                                                                                                                                                                                                                      | N/A                                                                                                                          |
| 3. Configure an IPv6 object policy rule. | <b>rule</b> [ <i>rule-id</i> ] { <b>drop</b>   <b>pass</b> } [ [ <b>source-ip</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>destination-ip</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>service</b> { <i>object-group-name</i>   <b>any</b> } ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>counting</b> ] [ <b>disable</b> ] [ <b>logging</b> ] [ <b>time-range</b> <i>time-range-name</i> ] ] * | By default, no object policy rule exists.<br><br>If you specify a nonexistent object group, the rule does not match packets. |
| 4. (Optional.) Configure a               | <b>rule</b> <i>rule-id</i> <b>comment</b> <i>text</i>                                                                                                                                                                                                                                                                                                                                                    | By default, an object policy rule                                                                                            |



| Step                      | Command | Remarks                      |
|---------------------------|---------|------------------------------|
| description for the rule. |         | does not have a description. |

## Applying object policies to zone pairs

You can apply one IPv4 object policy and one IPv6 object policy to each zone pair. Configuration fails if you apply more than one IPv4 or IPv6 object policy to a zone pair.

To apply an object policy to a zone pair:

| Step                                            | Command                                                                                                                                                                                                                                                                          | Remarks                                                                                                                  |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                           | <b>system-view</b>                                                                                                                                                                                                                                                               | N/A                                                                                                                      |
| 2. Configure the security zones.                | <b>security-zone name</b> <i>zone-name</i>                                                                                                                                                                                                                                       | By default, no security zone exists.<br>You can repeat this command to create multiple security zones.                   |
| 3. Create a zone pair and enter zone pair view. | <b>zone-pair security source</b> <i>source-zone-name</i><br><b>destination</b> <i>destination-zone-name</i>                                                                                                                                                                      | By default, no zone pair exists.<br>For more information about this command, see <i>Fundamentals Command Reference</i> . |
| 4. Apply an object policy to the zone pair.     | <ul style="list-style-type: none"> <li>Apply an IPv4 object policy to the zone pair:<br/><b>object-policy apply ip</b> <i>object-policy-name</i></li> <li>Apply an IPv6 object policy to the zone pair:<br/><b>object-policy apply ipv6</b> <i>object-policy-name</i></li> </ul> | By default, no object policy is applied to a zone pair.                                                                  |

## Changing the rule match order

The device matches packets against object policy rules in the order the rules were configured. You can change the rule match order by changing the position of an object policy rule in the rule list.

To change the rule match order:

| Step                           | Command                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.          | <b>system-view</b>                                                                                                                                                                                                                     |
| 2. Enter object policy view.   | <ul style="list-style-type: none"> <li>Enter IPv4 object policy view:<br/><b>object-policy ip</b> <i>object-policy-name</i></li> <li>Enter IPv6 object policy view:<br/><b>object-policy ipv6</b> <i>object-policy-name</i></li> </ul> |
| 3. Move an object policy rule. | <b>move rule</b> <i>rule-id</i> <b>before</b> <i>insert-rule-id</i>                                                                                                                                                                    |

## Enabling rule matching acceleration

This feature accelerates rule matching. It enhances connection establishment and packet forwarding performance, especially for a device using multiple rules to match first packets from multiple users.

To enable rule matching acceleration:

| Step                                  | Command                                                                                                                                                                                                                             | Remarks                                                                  |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| 1. Enter system view.                 | <b>system-view</b>                                                                                                                                                                                                                  | N/A                                                                      |
| 2. Enter object policy view.          | <ul style="list-style-type: none"><li>Enter IPv4 object policy view:<br/><b>object-policy ip</b> <i>object-policy-name</i></li><li>Enter IPv6 object policy view:<br/><b>object-policy ipv6</b> <i>object-policy-name</i></li></ul> | N/A                                                                      |
| 3. Enable rule matching acceleration. | <b>accelerate</b>                                                                                                                                                                                                                   | By default, rule matching acceleration is disabled for an object policy. |

## Displaying and maintaining object policies

Execute the **display** commands in any view.

| Task                                                                                                                           | Command                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display acceleration information for object policies (centralized devices in standalone mode).                                 | <b>display object-policy accelerate</b> { <b>summary</b> { <b>ip</b>   <b>ipv6</b> }   <b>verbose</b> { <b>ip</b> <i>object-policy-name</i>   <b>ipv6</b> <i>object-policy-name</i> } }                                                                     |
| Display acceleration information for object policies (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display object-policy accelerate</b> { <b>summary</b> { <b>ip</b>   <b>ipv6</b> }   <b>verbose</b> { <b>ip</b> <i>object-policy-name</i>   <b>ipv6</b> <i>object-policy-name</i> } <b>slot</b> <i>slot-number</i> }                                      |
| Display acceleration information for object policies (distributed devices in IRF mode).                                        | <b>display object-policy accelerate</b> { <b>summary</b> { <b>ip</b>   <b>ipv6</b> }   <b>verbose</b> { <b>ip</b> <i>object-policy-name</i>   <b>ipv6</b> <i>object-policy-name</i> } <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> } |
| Display information about IPv4 object policies.                                                                                | <b>display object-policy ip</b> [ <i>object-policy-name</i> ]                                                                                                                                                                                               |
| Display information about IPv6 object policies.                                                                                | <b>display object-policy ipv6</b> [ <i>object-policy-name</i> ]                                                                                                                                                                                             |
| Display information about the object policies applied to zone pairs.                                                           | <b>display object-policy zone-pair security</b> [ <b>source</b> <i>source-zone-name</i> <b>destination</b> <i>destination-zone-name</i> ]                                                                                                                   |
| Display statistics for object policies applied to a zone pair.                                                                 | <b>display object-policy statistics zone-pair security source</b> <i>source-zone-name</i> <b>destination</b> <i>destination-zone-name</i> [ <b>ip</b>   <b>ipv6</b> ]                                                                                       |
| Clear statistics for the object policies applied to zone pairs.                                                                | <b>reset object-policy statistics</b> [ <b>zone-pair security source</b> <i>source-zone-name</i> <b>destination</b> <i>destination-zone-name</i> ] [ <b>ip</b>   <b>ipv6</b> ]                                                                              |

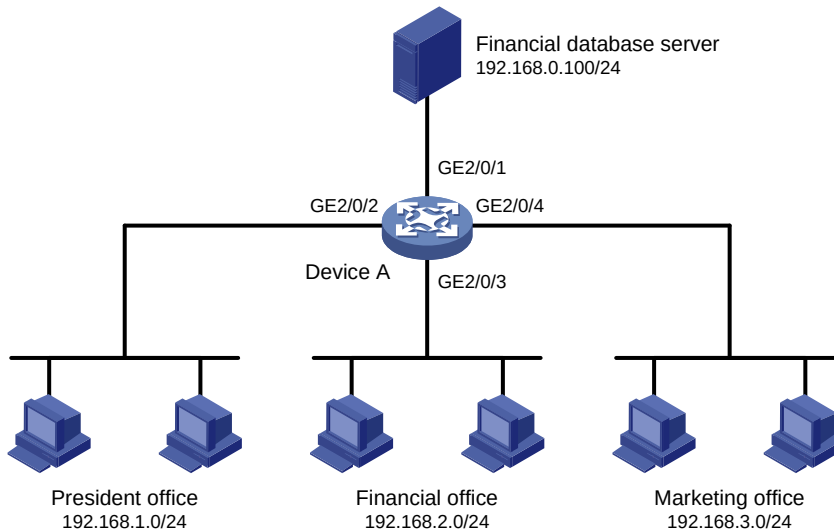
## Object policy configuration example

### Network requirements

Configure object policies to achieve the following goals:

- The president office can access the financial database server through HTTP at any time.
- The financial office can access the financial database server through HTTP from 8:00 to 18:00 on weekdays.
- The marketing office cannot access the financial database server through HTTP at any time.

Figure 147 Network diagram



## Configuration procedure

1. Create a time range named **work** to cover 8:00 to 18:00 on weekdays.  

```
<DeviceA> system-view
[DeviceA] time-range work 08:00 to 18:00 working-day
```
2. Create security zones:  
# Create a security zone named **president**, and add **GigabitEthernet 2/0/2** to the zone.  

```
[DeviceA] security-zone name president
[DeviceA-security-zone-president] import interface gigabitethernet 2/0/2
[DeviceA-security-zone-president] quit
```

  
# Create a security zone named **finance**, and add **GigabitEthernet 2/0/3** to the zone.  

```
[DeviceA] security-zone name finance
[DeviceA-security-zone-finance] import interface gigabitethernet 2/0/3
[DeviceA-security-zone-finance] quit
```

  
# Create a security zone named **market**, and add **GigabitEthernet 2/0/4** to the zone.  

```
[DeviceA] security-zone name market
[DeviceA-security-zone-market] import interface gigabitethernet 2/0/4
[DeviceA-security-zone-market] quit
```

  
# Create a security zone named **database**, and add **GigabitEthernet 2/0/1** to the zone.  

```
[DeviceA] security-zone name database
[DeviceA-security-zone-database] import interface gigabitethernet 2/0/1
[DeviceA-security-zone-database] quit
```
3. Create object groups:  
# Create an IPv4 address object group named **president**. Configure an IPv4 address object with the subnet address of **192.168.1.0/24** for the group.  

```
[DeviceA] object-group ip address president
[DeviceA-obj-grp-ip-president] network subnet 192.168.1.0 24
[DeviceA-obj-grp-ip-president] quit
```

  
# Create an IPv4 address object group named **finance**. Configure an IPv4 address object with the subnet address of **192.168.2.0/24** for the group.

```
[DeviceA] object-group ip address finance
[DeviceA-obj-grp-ip-finance] network subnet 192.168.2.0 24
[DeviceA-obj-grp-ip-finance] quit

Create an IPv4 address object group named market. Configure an IPv4 address object with
the subnet address of 192.168.3.0/24 for the group.
[DeviceA] object-group ip address market
[DeviceA-obj-grp-ip-market] network subnet 192.168.3.0 24
[DeviceA-obj-grp-ip-market] quit

Create an IPv4 address object group named database. Configure an IPv4 address object
with the subnet address of 192.168.0.0/24 for the group.
[DeviceA] object-group ip address database
[DeviceA-obj-grp-ip-database] network subnet 192.168.0.0 24
[DeviceA-obj-grp-ip-database] quit

Create a service object group named web. Configure a service object with the HTTP service.
[DeviceA] object-group service web
[DeviceA-obj-grp-service-web] service 6 destination eq 80
[DeviceA-obj-grp-service-web] quit
```

#### 4. Create object policies and rules:

# Create an IPv4 object policy named **president-database**. Configure a rule that allows the president office to access the financial database server through HTTP at any time.

```
[DeviceA] object-policy ip president-database
[DeviceA-object-policy-ip-president-database] rule pass source-ip president
destination-ip database service web
[DeviceA-object-policy-ip-president-database] quit
```

# Create an IPv4 object policy named **finance-database**. Configure a rule that allows the financial office to access the financial database server through HTTP from 8:00 to 18:00 on weekdays.

```
[DeviceA] object-policy ip finance-database
[DeviceA-object-policy-ip-finance-database] rule pass source-ip finance
destination-ip database service web time-range work
[DeviceA-object-policy-ip-finance-database] quit
```

# Create an IPv4 object policy named **market-database**. Configure a rule that prohibits the marketing office from accessing the financial database server through HTTP at any time.

```
[DeviceA] object-policy ip market-database
[DeviceA-object-policy-ip-market-database] rule drop source-ip market
destination-ip database service web
[DeviceA-object-policy-ip-market-database] quit
```

#### 5. Apply object policies to zone pairs:

# Create a zone pair from security zone **president** to security zone **database**. Apply IPv4 object policy **president-database** to the zone pair.

```
[DeviceA] zone-pair security source president destination database
[DeviceA-zone-pair-security-president-database] object-policy apply ip
president-database
[DeviceA-zone-pair-security-president-database] quit
```

# Create a zone pair from security zone **finance** to security zone **database**. Apply IPv4 object policy **finance-database** to the zone pair.

```
[DeviceA] zone-pair security source finance destination database
[DeviceA-zone-pair-security-finance-database] object-policy apply ip
finance-database
[DeviceA-zone-pair-security-finance-database] quit
```

```
Create a zone pair from security zone market to security zone database. Apply IPv4 object
policy market-database to the zone pair.
[DeviceA] zone-pair security source market destination database
[DeviceA-zone-pair-security-market-database] object-policy apply ip market-database
[DeviceA-zone-pair-security-market-database] quit
```

## Verifying the configuration

# Use a PC in each office to access the Web service of the financial database server through the browser. (Details not shown.)

# Configuring attack detection and prevention

## Overview

Attack detection and prevention enables a device to detect attacks by inspecting arriving packets, and to take prevention actions to protect a private network. Prevention actions include logging, packet dropping, blacklisting, and client verification.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Attacks that the device can prevent

The device can detect and prevent single-packet attacks, scanning attacks, and flood attacks.

### Single-packet attacks

Single-packet attacks are also known as malformed packet attacks. An attacker typically launches single-packet attacks by using the following methods:

- An attacker sends defective packets to a device, which causes the device to malfunction or crash.
- An attacker sends normal packets to a device, which interrupts connections or probes network topologies.
- An attacker sends a large number of forged packets to a target device, which consumes network bandwidth and causes denial of service (DoS).

[Table 14](#) lists the single-packet attack types that the device can detect and prevent.

**Table 14 Types of single-packet attacks**

| Single-packet attack         | Description                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ICMP redirect                | An attacker sends ICMP redirect messages to modify the victim's routing table. The victim cannot forward packets correctly. |
| ICMP destination unreachable | An attacker sends ICMP destination unreachable messages to cut off the connections between the victim and its destinations. |

| Single-packet attack | Description                                                                                                                                                                                                                                                                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP type            | A receiver responds to an ICMP packet according to its type. An attacker sends forged ICMP packets of a specific type to affect the packet processing of the victim.                                                                                                                                                                        |
| ICMPv6 type          | A receiver responds to an ICMPv6 packet according to its type. An attacker sends forged ICMPv6 packets of specific types to affect the packet processing of the victim.                                                                                                                                                                     |
| Land                 | An attacker sends the victim a large number of TCP SYN packets, which contain the victim's IP address as the source and destination IP addresses. This attack exhausts the half-open connection resources on the victim, and locks the victim's system.                                                                                     |
| Large ICMP packet    | An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.                                                                                                                                                                                                |
| Large ICMPv6 packet  | An attacker sends large ICMPv6 packets to crash the victim. Large ICMPv6 packets can cause memory allocation error and crash the protocol stack.                                                                                                                                                                                            |
| IP options           | An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.                                                                                                                                   |
| IP fragment          | An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.                                                                                                                                                                                              |
| IP impossible packet | An attacker sends IP packets whose source IP address is the same as the destination IP address, which causes the victim to malfunction.                                                                                                                                                                                                     |
| Tiny fragment        | An attacker makes the fragment size small enough to force Layer 4 header fields into the second fragment. These fragments can pass the packet filtering because they do not hit any match.                                                                                                                                                  |
| Smurf                | An attacker broadcasts an ICMP echo request to target networks. These requests contain the victim's IP address as the source IP address. Every receiver on the target networks will send an ICMP echo reply to the victim. The victim will be flooded with replies, and will be unable to provide services. Network congestion might occur. |
| TCP flag             | An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.                                                                          |
| Traceroute           | An attacker uses traceroute tools to probe the topology of the victim network.                                                                                                                                                                                                                                                              |
| WinNuke              | An attacker sends Out-Of-Band (OOB) data to the TCP port 139 (NetBIOS) on the victim that runs Windows system. The malicious packets contain the Urgent Pointer, which causes the victim's operating system to crash and display a Blue Screen of Death (BSOD).                                                                             |
| UDP bomb             | An attacker sends a malformed UDP packet. The length value in the IP header is larger than the IP header length plus the length value in the UDP header. When the target system processes the packet, a buffer overflow can occur, which causes a system crash.                                                                             |
| UDP Snork            | An attacker sends a UDP packet with destination port 135 (the Microsoft location service) and source port 135, 7, or 19. This attack causes an NT system to exhaust its CPU.                                                                                                                                                                |
| UDP Fraggle          | An attacker sends a large number of chargen packets with source UDP port 7 and destination UDP port 19 to a network. These packets use the victim's IP address as the source IP address. Replies will flood the victim, resulting in DoS.                                                                                                   |

| Single-packet attack | Description                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Teardrop             | An attacker sends a stream of overlapping fragments. The victim will crash when it tries to reassemble the overlapping fragments.                                                                          |
| Ping of death        | An attacker sends the victim an ICMP echo request larger than 65535 bytes that violates the IP protocol. When the victim reassembles the packet, a buffer overflow can occur, which causes a system crash. |

## Scanning attacks

Scanning is a preintrusion activity used to prepare for intrusion into a network. The scanning allows the attacker to find a way into the target network and to disguise the attacker's identity.

Attackers use scanning tools to probe a network, find vulnerable hosts, and discover services that are running on the hosts. Attackers can use the information to launch attacks.

The device can detect and prevent the IP sweep and port scan attacks. If an attacker performs port scanning from multiple hosts to the target host, distributed port scan attacks occur.

## Flood attacks

An attacker launches a flood attack by sending a large number of forged requests to the victim in a short period of time. The victim is too busy responding to these forged requests to provide services for legal users, and a DoS attack occurs.

The device can detect and prevent the following types of flood attacks:

- **SYN flood attack.**  
A SYN flood attacker exploits the TCP three-way handshake characteristics and makes the victim unresponsive to legal users. An attacker sends a large number of SYN packets with forged source addresses to a server. This causes the server to open a large number of half-open connections and respond to the requests. However, the server will never receive the expected ACK packets. The server is unable to accept new incoming connection requests because all of its resources are bound to half-open connections.
- **ACK flood attack.**  
An ACK packet is a TCP packet only with the ACK flag set. Upon receiving an ACK packet from a client, the server must search half-open connections for a match.  
An ACK flood attacker sends a large number of ACK packets to the server. This causes the server to be busy searching for half-open connections, and the server is unable to process packets for normal services.
- **SYN-ACK flood attack.**  
Upon receiving a SYN-ACK packet, the server must search for the matching SYN packet it has sent. A SYN-ACK flood attacker sends a large number of SYN-ACK packets to the server. This causes the server to be busy searching for SYN packets, and the server is unable to process packets for normal services.
- **FIN flood attack.**  
FIN packets are used to shut down TCP connections.  
A FIN flood attacker sends a large number of forged FIN packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections.
- **RST flood attack.**  
RST packets are used to abort TCP connections when TCP connection errors occur.



An RST flood attacker sends a large number of forged RST packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections.

- DNS flood attack.

The DNS server processes and replies all DNS queries that it receives.

A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

- HTTP flood attack.

Upon receiving an HTTP GET request, the HTTP server performs complex operations, including character string searching, database traversal, data reassembly, and format switching. These operations consume a large amount of system resources.

An HTTP flood attacker sends a large number of HTTP GET requests that exceed the processing capacity of the HTTP server, which causes the server to crash.

- ICMP flood attack.

An ICMP flood attacker sends ICMP request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services.

- ICMPv6 flood attack.

An ICMPv6 flood attacker sends ICMPv6 request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services.

- UDP flood attack.

A UDP flood attacker sends UDP packets to a host at a fast rate. These packets consume a large amount of the target host's bandwidth, so the host cannot provide other services.

## TCP fragment attacks

An attacker launches TCP fragment attacks by sending attack TCP fragments defined in RFC 1858:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

Typically, packet filter detects the source and destination IP addresses, source and destination ports, and transport layer protocol of the first fragment of a TCP packet. If the first fragment passes the detection, all subsequent fragments of the TCP packet are allowed to pass through.

Because the first fragment of attack TCP packets does not hit any match in the packet filter, the subsequent fragments can all pass through. After the receiving host reassembles the fragments, a TCP fragment attack occurs.

To prevent TCP fragment attacks, enable TCP fragment attack prevention to drop attack TCP fragments.

## Blacklist feature

The following matrix shows the feature and hardware compatibility:

| Hardware                             | Blacklist compatibility |
|--------------------------------------|-------------------------|
| MSR954(JH296A/JH297A/ JH298A/JH299A) | No                      |
| MSR1002-4/1003-8S                    | Yes                     |
| MSR2003                              | Yes                     |

| Hardware               | Blacklist compatibility |
|------------------------|-------------------------|
| MSR2004-24/2004-48     | Yes                     |
| MSR3012/3024/3044/3064 | Yes                     |
| MSR4060/4080           | Yes                     |

The blacklist feature is an attack prevention method that filters packets by source IP addresses in blacklist entries. Compared with ACL-based packet filter, blacklist filtering is simpler and provides effective screening at a faster speed.

## Client verification

### TCP client verification

The TCP client verification feature protects TCP servers against the following flood attacks:

- SYN.
- ACK.
- SYN-ACK.
- FIN.
- RST.

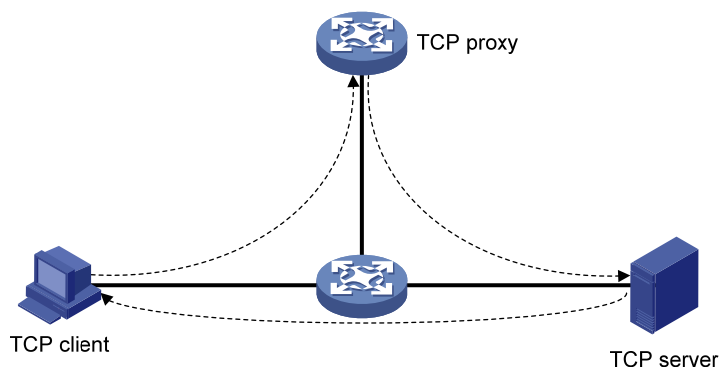
The TCP client verification feature enables a TCP proxy on the device.

TCP client verification can operate in the following modes:

- **Safe reset**—Enables unidirectional TCP proxy for packets only from TCP connection initiators. The unidirectional TCP proxy is sufficient for most scenarios because attacks are often seen from clients.

As shown in [Figure 148](#), if packets from TCP clients pass through the proxy device, but the packets from servers do not, only the safe reset mode can be used.

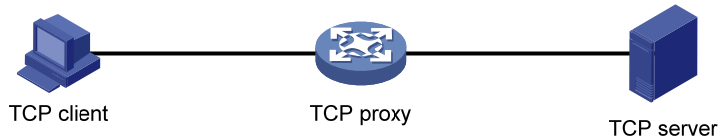
**Figure 148 Safe reset mode application**



- **SYN cookie**—Enables bidirectional TCP proxy for TCP clients and servers.

As shown in [Figure 149](#), if packets from clients and servers pass through the TCP proxy device, either safe reset or SYN cookie can be used.

**Figure 149 Safe reset/SYN cookie mode application**



### TCP proxy in safe reset mode

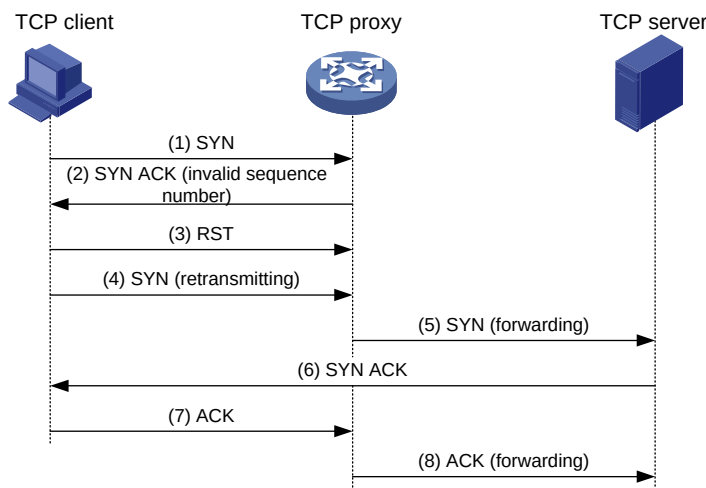
As shown in [Figure 150](#), the safe reset mode functions as follows:

1. After receiving a SYN packet destined for a protected server, the TCP proxy sends back a SYN ACK packet with an invalid sequence number.
2. If the TCP proxy receives an RST packet from the client, the client is verified as legitimate.
3. The TCP proxy adds the client's IP address to the trusted IP list and starts forwarding TCP packets from the client to the server.

The safe reset mode requires that TCP clients use the standard TCP protocol suite. Legitimate clients that use non-standard TCP protocol suites will be verified as illegitimate by the TCP proxy.

With client verification, the TCP connection establishment takes more time than normal TCP connection establishment.

**Figure 150 TCP proxy in safe reset mode**



### TCP proxy in SYN cookie mode

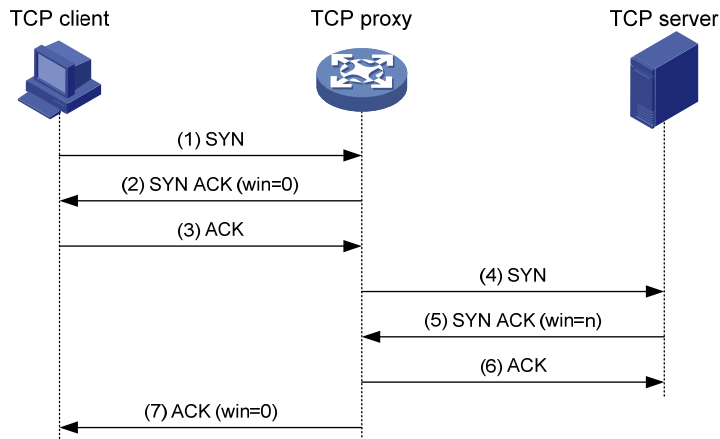
As shown in [Figure 151](#), SYN cookie mode requires two TCP connections to be established as follows:

1. After receiving a SYN packet from a client to a protected server, the TCP proxy sends back a SYN ACK packet with the window size 0. If the client responds with an ACK packet, the client is verified as legitimate. The proxy device establishes a TCP connection with the client.
2. The TCP proxy device establishes a connection with the server through a new three-way handshake that has a different window size. This connection uses a different sequence number from the connection between the client and proxy device.

In SYN cookie mode, the TCP proxy is the server proxy that communicates with clients and the client proxy that communicates with server. Choose this mode when the following requirements are met:

- The TCP proxy device is deployed on the key path that passes through the ingress and egress of the protected server.
- All packets exchanged between clients and server pass through the TCP proxy device.

**Figure 151 TCP proxy in SYN cookie mode**



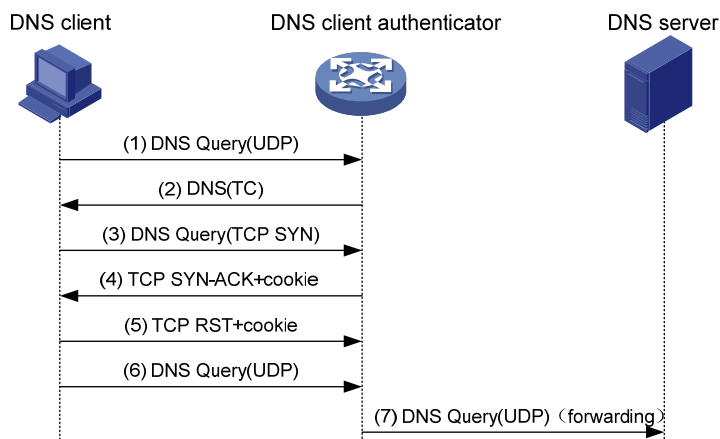
## DNS client verification

The DNS client verification feature protects DNS servers against DNS flood attacks. It is configured on the device where packets from the DNS clients to the DNS servers pass through. The device with DNS client verification feature configured is called a DNS client authenticator.

As shown in [Figure 152](#), the DNS client verification functions as follows:

1. Upon receiving a UDP DNS query destined for a protected server, the DNS client authenticator responds with a DNS truncate (TC) packet. The DNS truncate packet requires the client to initiate a query in a TCP packet.
2. When the authenticator receives a DNS query in a TCP SYN packet to port 53 from the client, the authenticator responds with a SYN-ACK packet.
3. When the authenticator receives a RST packet from the client, the authenticator verifies the client as legitimate.
4. The authenticator adds the client's IP address to the trusted IP list and forwards the trusted client's subsequent packets to the server.

**Figure 152 DNS client verification process**



The DNS client verification feature requires that clients use the standard TCP/IP protocol suite and DNS protocol. Legitimate clients that use non-standard protocols will be verified as illegitimate by the DNS client authenticator.

With client verification, the first DNS resolution takes more time than normal DNS resolution.

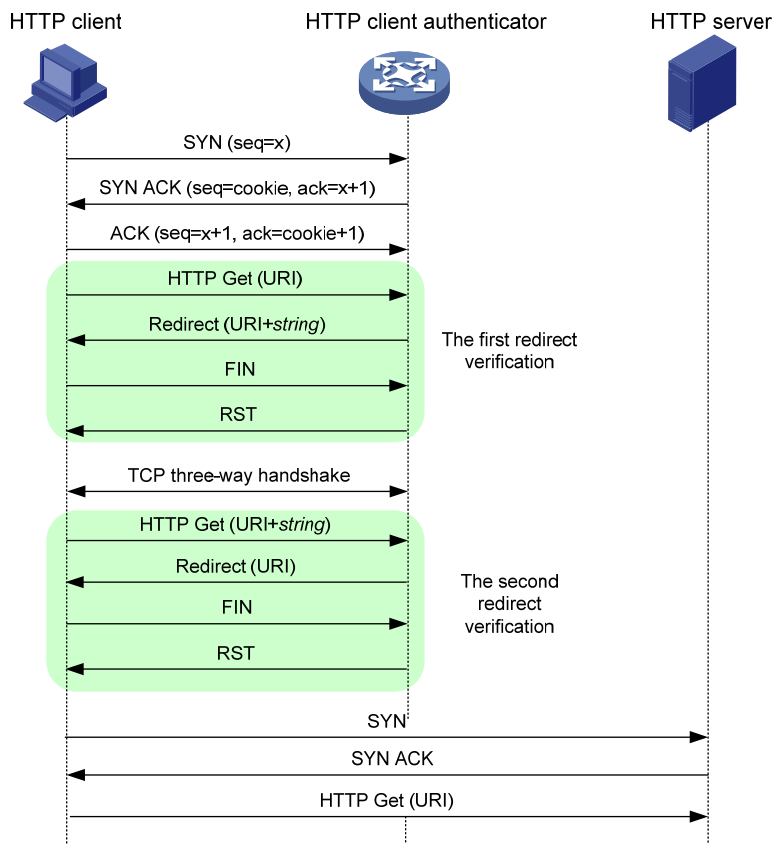
# HTTP client verification

The HTTP client verification feature protects HTTP servers against HTTP flood attacks. It is configured on the device where packets from the HTTP clients to the HTTP servers pass through. A device with HTTP client verification feature configured is called an HTTP client authenticator.

As shown in [Figure 153](#), the HTTP client verification functions as follows:

1. Upon receiving a SYN packet destined for a protected HTTP server, the HTTP client authenticator performs TCP client verification in SYN cookie mode. If the client passes the TCP client verification, a TCP connection is established between the client and the authenticator. For more information about TCP client verification, see "[TCP client verification](#)."
2. When the authenticator receives an HTTP Get packet from the client, it performs the first redirect verification. The authenticator records the client information and responds with an HTTP Redirect packet. The HTTP Redirect packet contains a redirect URI and requires the client to terminate the TCP connection.
3. After receiving the HTTP Redirect packet, the client terminates the TCP connection and then establishes a new TCP connection with the authenticator.
4. When the authenticator receives the HTTP Get packet, it performs the second redirection verification. The authenticator verifies the following information:
  - The client has passed the first redirection verification.
  - The URI in the HTTP Get packet is the redirect URI.
5. If the client passes the second redirection verification, the authenticator adds its IP address to the trusted IP list, and responds a Redirect packet. The Redirect packet contains the URI that the client originally carried and requires the client to terminate the TCP connection.
6. The authenticator directly forwards the trusted client's subsequent packets to the server.

**Figure 153 HTTP client verification process**



# Attack detection and prevention configuration task list

| Tasks at a glance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Required.) <a href="#">Configuring an attack defense policy</a> : <ul style="list-style-type: none"><li>• (Required.) <a href="#">Creating an attack defense policy</a></li><li>• (Required.) Perform at least one of the following tasks to configure attack detection:<ul style="list-style-type: none"><li>◦ <a href="#">Configuring a single-packet attack defense policy</a></li><li>◦ <a href="#">Configuring a scanning attack defense policy</a></li><li>◦ <a href="#">Configuring a flood attack defense policy</a></li></ul></li><li>• (Optional.) <a href="#">Configuring attack detection exemption</a></li></ul> |
| (Required.) Perform at least one of the tasks to apply an attack defense policy: <ul style="list-style-type: none"><li>• <a href="#">Applying an attack defense policy to an interface</a></li><li>• <a href="#">Applying an attack defense policy to the device</a></li></ul>                                                                                                                                                                                                                                                                                                                                                 |
| (Optional.) <a href="#">Disabling log aggregation for single-packet attack events</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| (Optional.) <a href="#">Configuring TCP fragment attack prevention</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| (Optional.) Configuring client verification: <ul style="list-style-type: none"><li>• <a href="#">Configuring TCP client verification</a></li><li>• <a href="#">Configuring DNS client verification</a></li><li>• <a href="#">Configuring HTTP client verification</a></li></ul>                                                                                                                                                                                                                                                                                                                                                |
| (Optional.) <a href="#">Configuring the blacklist feature</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring an attack defense policy

### Creating an attack defense policy

An attack defense policy can contain a set of attack detection and prevention configuration against multiple attacks.

To create an attack defense policy:

| Step                                                   | Command                                            | Remarks                                      |
|--------------------------------------------------------|----------------------------------------------------|----------------------------------------------|
| 1. Enter system view.                                  | <b>system-view</b>                                 | N/A                                          |
| 2. Create an attack defense policy and enter its view. | <b>attack-defense policy</b><br><i>policy-name</i> | By default, no attack defense policy exists. |

### Configuring a single-packet attack defense policy

Configure the single-packet attack defense policy on the interface that connects to the external network.

Single-packet attack detection inspects incoming packets based on the packet signature. If an attack packet is detected, the device can take the following actions:

- Output logs (the default action).
- Drop attack packets.

You can also configure the device to not take any actions.

To configure a single-packet attack defense policy:

| Step                                                                  | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Remarks                                                                                                                                                                                                   |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                 | <b>system-view</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | N/A                                                                                                                                                                                                       |
| 2. Enter attack defense policy view.                                  | <b>attack-defense policy</b> <i>policy-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | N/A                                                                                                                                                                                                       |
| 3. Configure signature detection for single-packet attacks.           | <ul style="list-style-type: none"> <li><b>signature detect</b> { <b>fraggle</b>   <b>fragment</b>   <b>impossible</b>   <b>ip-option-abnormal</b>   <b>land</b>   <b>large-icmp</b>   <b>large-icmpv6</b>   <b>ping-of-death</b>   <b>smurf</b>   <b>snork</b>   <b>tcp-all-flags</b>   <b>tcp-fin-only</b>   <b>tcp-invalid-flags</b>   <b>tcp-null-flag</b>   <b>tcp-syn-fin</b>   <b>teardrop</b>   <b>tiny-fragment</b>   <b>traceroute</b>   <b>udp-bomb</b>   <b>winnuke</b> } [ <b>action</b> { { <b>drop</b>   <b>logging</b> } *   <b>none</b> } ]</li> <li><b>signature detect icmp-type</b> { <i>icmp-type-value</i>   <b>address-mask-reply</b>   <b>address-mask-request</b>   <b>destination-unreachable</b>   <b>echo-reply</b>   <b>echo-request</b>   <b>information-reply</b>   <b>information-request</b>   <b>parameter-problem</b>   <b>redirect</b>   <b>source-quench</b>   <b>time-exceeded</b>   <b>timestamp-reply</b>   <b>timestamp-request</b> } [ <b>action</b> { { <b>drop</b>   <b>logging</b> } *   <b>none</b> } ]</li> <li><b>signature detect icmpv6-type</b> { <i>icmpv6-type-value</i>   <b>destination-unreachable</b>   <b>echo-reply</b>   <b>echo-request</b>   <b>group-query</b>   <b>group-reduction</b>   <b>group-report</b>   <b>packet-too-big</b>   <b>parameter-problem</b>   <b>time-exceeded</b> } [ <b>action</b> { { <b>drop</b>   <b>logging</b> } *   <b>none</b> } ]</li> <li><b>signature detect ip-option</b> { <i>option-code</i>   <b>internet-timestamp</b>   <b>loose-source-routing</b>   <b>record-route</b>   <b>route-alert</b>   <b>security</b>   <b>stream-id</b>   <b>strict-source-routing</b> } [ <b>action</b> { { <b>drop</b>   <b>logging</b> } *   <b>none</b> } ]</li> </ul> | <p>By default, signature detection is not configured for single-packet attacks.</p> <p>You can configure signature detection for multiple single-packet attacks.</p>                                      |
| 4. (Optional.) Set the maximum length of safe ICMP or ICMPv6 packets. | <b>signature</b> { <b>large-icmp</b>   <b>large-icmpv6</b> } <b>max-length</b> <i>length</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>By default, the maximum length of safe ICMP or ICMPv6 packets is 4000 bytes.</p> <p>A large ICMP or ICMPv6 attack occurs if an ICMP or ICMPv6 packet larger than the specified length is detected.</p> |

| Step                                                                                     | Command                                                                                      | Remarks                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. (Optional.) Specify the actions against single-packet attacks of a specific level.    | <b>signature level { high   info   low   medium } action { { drop   logging } *   none }</b> | The default action is <b>logging</b> for single-packet attacks of the informational and low levels.<br>The default actions are <b>logging</b> and <b>drop</b> for single-packet attacks of the medium and high levels. |
| 6. (Optional.) Enable signature detection for single-packet attacks of a specific level. | <b>signature level { high   info   low   medium } detect</b>                                 | By default, signature detection is disabled for all levels of single-packet attacks.                                                                                                                                   |

## Configuring a scanning attack defense policy

Configure a scanning attack defense policy on the interface that connects to the external network.

Scanning attack detection inspects the incoming packet rate of connections to the target system. If a suspected source initiates connections at a rate equal to or exceeding the pre-defined threshold, the device can take the following actions:

- Output logs.
- Add the attacker's IP address to the blacklist.

To make the blacklist feature take effect, enable the blacklist feature globally or on the interface where the defense policy is applied. For more information about the blacklist feature, see "[Configuring the blacklist feature](#)."

To configure a scanning attack defense policy:

| Step                                    | Command                                                                                                  | Remarks                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 1. Enter system view.                   | <b>system-view</b>                                                                                       | N/A                                                      |
| 2. Enter attack defense policy view.    | <b>attack-defense policy</b><br><i>policy-name</i>                                                       | N/A                                                      |
| 3. Configure scanning attack detection. | <b>scan detect level { high   low   medium } action { block-source [ timeout minutes ]   logging } *</b> | By default, scanning attack detection is not configured. |

## Configuring a flood attack defense policy

Configure a flood attack defense policy on the interface that connects to the external network to protect internal servers.

Flood attack detection monitors the rate at which connections are initiated to the internal servers.

With flood attack detection enabled, the device is in attack detection state. An attack occurs when the device detects that the packet sending rate to a protected IP address reaches or exceeds the threshold. The device enters prevention state, and takes actions to protect the target IP address. When the rate is below the silence threshold (three-fourths of the threshold), the threat is over, and the device returns to the attack detection state.

If a device has multiple service cards, the global trigger threshold specified for preventing a flood attack is the global trigger threshold on each service card. When the policy is applied to the device, the global trigger threshold is the product of multiplying the specified threshold by the service card quantity.



You can configure flood attack detection and prevention for a specific IP address. For non-specific IP addresses, the device uses the global attack prevention settings.

### Configuring a SYN flood attack defense policy

| Step                                                                 | Command                                                                                                                                                                                       | Remarks                                                                           |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                                                                                                            | N/A                                                                               |
| 2. Enter attack defense policy view.                                 | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                            | N/A                                                                               |
| 3. Enable SYN flood attack detection for non-specific IP addresses.  | <b>syn-flood detect non-specific</b>                                                                                                                                                          | By default, SYN flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for SYN flood attack prevention. | <b>syn-flood threshold</b><br><i>threshold-value</i>                                                                                                                                          | By default, the global trigger threshold is 1000 for SYN flood attack prevention. |
| 5. Specify global actions against SYN flood attacks.                 | <b>syn-flood action { client-verify   drop   logging } *</b>                                                                                                                                  | By default, no global action is specified for SYN flood attacks.                  |
| 6. Configure IP-specific SYN flood attack detection.                 | <b>syn-flood detect { ip ip-address   ipv6 ipv6-address }<br/>[ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify   drop   logging } *   none } ]</b> | By default, SYN flood attack detection is not configured for any IP address.      |

### Configuring an ACK flood attack defense policy

| Step                                                                 | Command                                                                                                                                                                                       | Remarks                                                                           |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                                                                                                            | N/A                                                                               |
| 2. Enter attack defense policy view.                                 | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                            | N/A                                                                               |
| 3. Enable ACK flood attack detection for non-specific IP addresses.  | <b>ack-flood detect non-specific</b>                                                                                                                                                          | By default, ACK flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for ACK flood attack prevention. | <b>ack-flood threshold</b><br><i>threshold-value</i>                                                                                                                                          | By default, the global trigger threshold is 1000 for ACK flood attack prevention. |
| 5. Specify global actions against ACK flood attacks.                 | <b>ack-flood action { client-verify   drop   logging } *</b>                                                                                                                                  | By default, no global action is specified for ACK flood attacks.                  |
| 6. Configure IP-specific ACK flood attack detection.                 | <b>ack-flood detect { ip ip-address   ipv6 ipv6-address }<br/>[ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify   drop   logging } *   none } ]</b> | By default, ACK flood attack detection is not configured for any IP address.      |

### Configuring a SYN-ACK flood attack defense policy

| Step                  | Command            | Remarks |
|-----------------------|--------------------|---------|
| 1. Enter system view. | <b>system-view</b> | N/A     |

| Step                                                                     | Command                                                                                                                                                                                                                                                                                     | Remarks                                                                               |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 2. Enter attack defense policy view.                                     | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                                                                                                                          | N/A                                                                                   |
| 3. Enable SYN-ACK flood attack detection for non-specific IP addresses.  | <b>syn-ack-flood detect non-specific</b>                                                                                                                                                                                                                                                    | By default, SYN-ACK flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for SYN-ACK flood attack prevention. | <b>syn-ack-flood threshold</b><br><i>threshold-value</i>                                                                                                                                                                                                                                    | By default, the global trigger threshold is 1000 for SYN-ACK flood attack prevention. |
| 5. Specify global actions against SYN-ACK flood attacks.                 | <b>syn-ack-flood action</b><br>{ <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *                                                                                                                                                                                                    | By default, no global action is specified for SYN-ACK flood attacks.                  |
| 6. Configure IP-specific SYN-ACK flood attack detection.                 | <b>syn-ack-flood detect</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, SYN-ACK flood attack detection is not configured for any IP address.      |

### Configuring a FIN flood attack defense policy

| Step                                                                 | Command                                                                                                                                                                                                                                                                                 | Remarks                                                                           |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                                                                                                                                                                                                      | N/A                                                                               |
| 2. Enter attack defense policy view.                                 | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                                                                                                                      | N/A                                                                               |
| 3. Enable FIN flood attack detection for non-specific IP addresses.  | <b>fin-flood detect non-specific</b>                                                                                                                                                                                                                                                    | By default, FIN flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for FIN flood attack prevention. | <b>fin-flood threshold</b><br><i>threshold-value</i>                                                                                                                                                                                                                                    | By default, the global trigger threshold is 1000 for FIN flood attack prevention. |
| 5. Specify global actions against FIN flood attacks.                 | <b>fin-flood action</b> { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *                                                                                                                                                                                                       | By default, no global action is specified for FIN flood attacks.                  |
| 6. Configure IP-specific FIN flood attack detection.                 | <b>fin-flood detect</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, FIN flood attack detection is not configured for any IP address.      |

### Configuring an RST flood attack defense policy

| Step                                                                | Command                                            | Remarks                                                                           |
|---------------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                               | <b>system-view</b>                                 | N/A                                                                               |
| 2. Enter attack defense policy view.                                | <b>attack-defense policy</b><br><i>policy-name</i> | N/A                                                                               |
| 3. Enable RST flood attack detection for non-specific IP addresses. | <b>rst-flood detect non-specific</b>               | By default, RST flood attack detection is disabled for non-specific IP addresses. |

| Step                                                                 | Command                                                                                                                                                                                                                                                                                 | Remarks                                                                           |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 4. Set the global trigger threshold for RST flood attack prevention. | <b>rst-flood threshold</b><br><i>threshold-value</i>                                                                                                                                                                                                                                    | By default, the global trigger threshold is 1000 for RST flood attack prevention. |
| 5. Specify global actions against RST flood attacks.                 | <b>rst-flood action</b> { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *                                                                                                                                                                                                       | By default, no global action is specified for RST flood attacks.                  |
| 6. Configure IP-specific RST flood attack detection.                 | <b>rst-flood detect</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, RST flood attack detection is not configured for any IP address.      |

### Configuring an ICMP flood attack defense policy

| Step                                                                  | Command                                                                                                                                                                                                              | Remarks                                                                            |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 1. Enter system view.                                                 | <b>system-view</b>                                                                                                                                                                                                   | N/A                                                                                |
| 2. Enter attack defense policy view.                                  | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                                                   | N/A                                                                                |
| 3. Enable ICMP flood attack detection for non-specific IP addresses.  | <b>icmp-flood detect non-specific</b>                                                                                                                                                                                | By default, ICMP flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for ICMP flood attack prevention. | <b>icmp-flood threshold</b><br><i>threshold-value</i>                                                                                                                                                                | By default, the global trigger threshold is 1000 for ICMP flood attack prevention. |
| 5. Specify global actions against ICMP flood attacks.                 | <b>icmp-flood action</b> { <b>drop</b>   <b>logging</b> } *                                                                                                                                                          | By default, no global action is specified for ICMP flood attacks.                  |
| 6. Configure IP-specific ICMP flood attack detection.                 | <b>icmp-flood detect ip</b> <i>ip-address</i><br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, ICMP flood attack detection is not configured for any IP address.      |

### Configuring an ICMPv6 flood attack defense policy

| Step                                                                     | Command                                                       | Remarks                                                                                |
|--------------------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 1. Enter system view.                                                    | <b>system-view</b>                                            | N/A                                                                                    |
| 2. Enter attack defense policy view.                                     | <b>attack-defense policy</b><br><i>policy-name</i>            | N/A                                                                                    |
| 3. Enable ICMPv6 flood attack detection for non-specific IPv6 addresses. | <b>icmpv6-flood detect non-specific</b>                       | By default, ICMPv6 flood attack detection is disabled for non-specific IPv6 addresses. |
| 4. Set the global trigger threshold for ICMPv6 flood attack prevention.  | <b>icmpv6-flood threshold</b><br><i>threshold-value</i>       | By default, the global trigger threshold is 1000 for ICMPv6 flood attack prevention.   |
| 5. Specify global actions against ICMPv6 flood attacks.                  | <b>icmpv6-flood action</b> { <b>drop</b>   <b>logging</b> } * | By default, no global action is specified for ICMPv6 flood attacks.                    |

| Step                                                    | Command                                                                                                                                                                                                                             | Remarks                                                                           |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 6. Configure IP-specific ICMPv6 flood attack detection. | <b>icmpv6-flood detect ipv6</b><br><i>ipv6-address</i> [ <b>vpn-instance</b><br><i>vpn-instance-name</i> ] [ <b>threshold</b><br><i>threshold-value</i> ] [ <b>action</b> { { <b>drop</b><br>  <b>logging</b> } *   <b>none</b> } ] | By default, ICMPv6 flood attack detection is not configured for any IPv6 address. |

### Configuring a UDP flood attack defense policy

| Step                                                                 | Command                                                                                                                                                                                                                                                                      | Remarks                                                                           |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                                | <b>system-view</b>                                                                                                                                                                                                                                                           | N/A                                                                               |
| 2. Enter attack defense policy view.                                 | <b>attack-defense policy</b><br><i>policy-name</i>                                                                                                                                                                                                                           | N/A                                                                               |
| 3. Enable UDP flood attack detection for non-specific IP addresses.  | <b>udp-flood detect non-specific</b>                                                                                                                                                                                                                                         | By default, UDP flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for UDP flood attack prevention. | <b>udp-flood threshold</b><br><i>threshold-value</i>                                                                                                                                                                                                                         | By default, the global trigger threshold is 1000 for UDP flood attack prevention. |
| 5. Specify global actions against UDP flood attacks.                 | <b>udp-flood action</b> { <b>drop</b>   <b>logging</b> } *                                                                                                                                                                                                                   | By default, no global action is specified for UDP flood attacks.                  |
| 6. Configure IP-specific UDP flood attack detection.                 | <b>udp-flood detect</b> { <b>ip</b> <i>ip-address</i><br>  <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b><br><i>vpn-instance-name</i> ] [ <b>threshold</b><br><i>threshold-value</i> ] [ <b>action</b> { { <b>drop</b><br>  <b>logging</b> } *   <b>none</b> } ] | By default, UDP flood attack detection is not configured for any IP address.      |

### Configuring a DNS flood attack defense policy

| Step                                                                               | Command                                                                           | Remarks                                                                           |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1. Enter system view.                                                              | <b>system-view</b>                                                                | N/A                                                                               |
| 2. Enter attack defense policy view.                                               | <b>attack-defense policy</b><br><i>policy-name</i>                                | N/A                                                                               |
| 3. Enable DNS flood attack detection for non-specific IP addresses.                | <b>dns-flood detect non-specific</b>                                              | By default, DNS flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for DNS flood attack prevention.               | <b>dns-flood threshold</b><br><i>threshold-value</i>                              | By default, the global trigger threshold is 1000 for DNS flood attack prevention. |
| 5. (Optional.) Specify the global ports to be protected against DNS flood attacks. | <b>dns-flood port</b> <i>port-list</i>                                            | By default, DNS flood attack prevention protects port 53.                         |
| 6. Specify global actions against DNS flood attacks.                               | <b>dns-flood action</b> { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } * | By default, no global action is specified for DNS flood attacks.                  |

| Step                                                 | Command                                                                                                                                                                                                                                                                                                                  | Remarks                                                                      |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 7. Configure IP-specific DNS flood attack detection. | <b>dns-flood detect</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>port</b> <i>port-list</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, DNS flood attack detection is not configured for any IP address. |

## Configuring an HTTP flood attack defense policy

| Step                                                                                | Command                                                                                                                                                                                                                                                                                                                   | Remarks                                                                            |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 1. Enter system view.                                                               | <b>system-view</b>                                                                                                                                                                                                                                                                                                        | N/A                                                                                |
| 2. Enter attack defense policy view.                                                | <b>attack-defense policy</b> <i>policy-name</i>                                                                                                                                                                                                                                                                           | N/A                                                                                |
| 3. Enable HTTP flood attack detection for non-specific IP addresses.                | <b>http-flood detect non-specific</b>                                                                                                                                                                                                                                                                                     | By default, HTTP flood attack detection is disabled for non-specific IP addresses. |
| 4. Set the global trigger threshold for HTTP flood attack prevention.               | <b>http-flood threshold</b> <i>threshold-value</i>                                                                                                                                                                                                                                                                        | By default, the global trigger threshold is 1000 for HTTP flood attack prevention. |
| 5. (Optional.) Specify the global ports to be protected against HTTP flood attacks. | <b>http-flood port</b> <i>port-list</i>                                                                                                                                                                                                                                                                                   | By default, HTTP flood attack prevention protects port 80.                         |
| 6. Specify global actions against HTTP flood attacks.                               | <b>http-flood action</b> { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *                                                                                                                                                                                                                                        | By default, no global action is specified for HTTP flood attacks.                  |
| 7. Configure IP-specific HTTP flood attack detection.                               | <b>http-flood detect</b> { <b>ip</b> <i>ip-address</i>   <b>ipv6</b> <i>ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>port</b> <i>port-list</i> ] [ <b>threshold</b> <i>threshold-value</i> ] [ <b>action</b> { { <b>client-verify</b>   <b>drop</b>   <b>logging</b> } *   <b>none</b> } ] | By default, HTTP flood attack detection is not configured for any IP address.      |

## Configuring attack detection exemption

The attack defense policy uses the ACL to identify exempted packets. The policy does not check the packets permitted by the ACL. You can configure the ACL to identify packets from trusted servers. The exemption feature reduces the false alarm rate and improves packet processing efficiency. For example, the attack defense policy identifies multicast packets with the same source addresses and different destination addresses, such as OSPF or PIM packets, as scanning attack packets. You can configure an ACL to exempt such packets from attack detection.

If an ACL is used for attack detection exemption, only the following match criteria in the ACL permit rules take effect:

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Protocol.

- L3VPN instance.
- **fragment** keyword for matching non-first fragments.

To configure attack detection exemption:

| Step                                     | Command                                                                                  | Remarks                                                                |
|------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1. Enter system view.                    | <b>system-view</b>                                                                       | N/A                                                                    |
| 2. Enter attack defense policy view.     | <b>attack-defense policy</b><br><i>policy-name</i>                                       | N/A                                                                    |
| 3. Configure attack detection exemption. | <b>exempt acl</b> [ <b>ipv6</b> ] { <i>acl-number</i><br>  <b>name</b> <i>acl-name</i> } | By default, the attack defense policy applies to all incoming packets. |

## Applying an attack defense policy to an interface

An attack defense policy does not take effect unless you apply it to an interface.

If you apply an attack defense policy to a global interface, specify a service card to process traffic for the interface. Otherwise, the policy cannot correctly detect and prevent scanning and flood attacks.

To apply an attack defense policy to an interface:

| Step                                                            | Command                                                           | Remarks                                                                  |
|-----------------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------|
| 1. Enter system view.                                           | <b>system-view</b>                                                | N/A                                                                      |
| 2. Enter system view.                                           | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                                                      |
| 3. Apply an attack defense policy to the interface.             | <b>attack-defense apply policy</b><br><i>policy-name</i>          | By default, no attack defense policy is applied to the interface.        |
| 4. Specify a service card to process traffic for the interface. | <b>service slot</b> <i>slot-number</i>                            | Optional.<br>By default, no service card is specified for the interface. |

## Applying an attack defense policy to the device

If you apply an attack defense policy to a device, the policy takes effect on packets destined for the device.

Applying an attack defense policy to a device improves the efficiency of processing attack packets destined for the device.

To apply an attack defense policy to the device:

| Step                                             | Command                                                     | Remarks                                                        |
|--------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------|
| 1. Enter system view.                            | <b>system-view</b>                                          | N/A                                                            |
| 2. Apply an attack defense policy to the device. | <b>attack-defense local apply policy</b> <i>policy-name</i> | By default, no attack defense policy is applied to the device. |

## Disabling log aggregation for single-packet attack events

Log aggregation aggregates all logs generated in a period and sends one log. The logs with the same attributes for the following items can be aggregated:

- Interface where the attack is detected.
- Attack type.
- Attack defense action.
- Source and destination IP addresses.
- VPN instance to which the victim IP address belongs.

As a best practice, do not disable log aggregation. A large number of logs will consume the display resources of the console.

To disable log aggregation for single-packet attack events:

| Step                                                        | Command                                           | Remarks                                                                 |
|-------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------|
| 1. Enter system view.                                       | <b>system-view</b>                                | N/A                                                                     |
| 2. Disable log aggregation for single-packet attack events. | <b>attack-defense signature log non-aggregate</b> | By default, log aggregation is enabled for single-packet attack events. |

## Configuring TCP fragment attack prevention

The TCP fragment attack prevention feature detects the length and fragment offset of received TCP fragments and drops attack TCP fragments.

TCP fragment attack prevention takes precedence over single-packet attack prevention. When both are used, incoming TCP packets are processed first by TCP fragment attack prevention and then by the single-packet attack defense policy.

To configure TCP fragment attack prevention:

| Step                                      | Command                                   | Remarks                                                                                                           |
|-------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                     | <b>system-view</b>                        | N/A                                                                                                               |
| 2. Enable TCP fragment attack prevention. | <b>attack-defense tcp fragment enable</b> | By default, TCP fragment attack prevention is enabled.<br>TCP fragment attack prevention is typically used alone. |

## Configuring TCP client verification

Configure TCP client verification on the interface that connects to the external network. TCP client verification protects internal TCP servers against TCP flood attacks, including the following flood attacks:

- SYN.
- SYN-ACK.
- RST.
- FIN.
- ACK.

IP addresses protected by TCP client verification can be manually added or automatically learned:

- You can manually add protected IP addresses. The device performs client verification when it receives the first SYN packet destined for a protected IP address.
- The TCP client verification can automatically add victims' IP addresses to the protected IP list when collaborating with flood attack detection. Make sure **client-verify** is specified as the flood attack prevention action. For more information, see "[Configuring a flood attack defense policy](#)."

If a TCP client is verified legitimate, the device adds the client's IP address to the trusted IP list. The device directly forwards TCP packets from trusted IP addresses.

To configure TCP client verification:

| Step                                                                                         | Command                                                                                                                                                                                                                         | Remarks                                                                                                                                                                |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                                        | <b>system-view</b>                                                                                                                                                                                                              | N/A                                                                                                                                                                    |
| 2. (Optional.) Specify an IP address to be protected by the TCP client verification feature. | <b>client-verify tcp protected { ip destination-ip-address   ipv6 destination-ipv6-address } [ vpn-instance vpn-instance-name ] [ port port-number ]</b>                                                                        | By default, the TCP client verification feature does not protect any IP address.                                                                                       |
| 3. Enter interface view.                                                                     | <b>interface interface-type interface-number</b>                                                                                                                                                                                | N/A                                                                                                                                                                    |
| 4. Enable TCP client verification on the interface.                                          | <ul style="list-style-type: none"><li>• To set the safe reset mode:<br/><b>client-verify tcp enable mode safe-reset</b></li><li>• To set the SYN cookie mode:<br/><b>client-verify tcp enable [ mode syn-cookie ]</b></li></ul> | By default, TCP client verification is disabled on the interface.<br><br>TCP client verification can be used alone or together with a TCP flood attack defense policy. |

## Configuring DNS client verification

Configure DNS client verification the interface that connects to the external network. The DNS client verification protects internal DNS servers against DNS flood attacks.

IP addresses protected by DNS client verification can be manually added or automatically learned:

- You can manually add protected IP addresses. The device performs client verification when it receives the first DNS query destined for a protected IP address.
- The DNS client verification can automatically add victims' IP addresses to the protected IP list when collaborating with DNS flood attack detection. Make sure **client-verify** is specified as the DNS flood attack prevention action. For more information, see "[Configuring a DNS flood attack defense policy](#)."

If a DNS client is verified legitimate, the device adds the client's IP address to the trusted IP list. The device directly forwards DNS packets from trusted IP addresses.

To configure DNS client verification:

| Step                                                                                         | Command                                                                                                                                                  | Remarks                                                                          |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 1. Enter system view.                                                                        | <b>system-view</b>                                                                                                                                       | N/A                                                                              |
| 2. (Optional.) Specify an IP address to be protected by the DNS client verification feature. | <b>client-verify dns protected { ip destination-ip-address   ipv6 destination-ipv6-address } [ vpn-instance vpn-instance-name ] [ port port-number ]</b> | By default, the DNS client verification feature does not protect any IP address. |



| Step                                                | Command                                                           | Remarks                                                                                                                                                                |
|-----------------------------------------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Enter interface view.                            | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                                                                                                                                                    |
| 4. Enable DNS client verification on the interface. | <b>client-verify dns enable</b>                                   | By default, DNS client verification is disabled on the interface.<br><br>DNS client verification can be used alone or together with a DNS flood attack defense policy. |

## Configuring HTTP client verification

Configure HTTP client verification on the interface that connects to the external network. The HTTP client verification protects internal HTTP servers against HTTP flood attacks.

IP addresses protected by HTTP client verification can be manually added or automatically learned:

- You can manually add protected IP addresses. The device performs client verification when it receives the first HTTP Get packet destined for a protected IP address.
- The HTTP client verification can automatically add victims' IP addresses to the protected IP list when collaborating with HTTP flood attack detection. Make sure **client-verify** is specified as the HTTP flood attack prevention action. For more information, see "[Configuring an HTTP flood attack defense policy](#)."

If an HTTP client is verified legitimate, the device adds the client's IP address to the trusted IP list. The device directly forwards HTTP packets from trusted IP addresses.

To configure HTTP client verification:

| Step                                                                                          | Command                                                                                                                                                                                                              | Remarks                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                                         | <b>system-view</b>                                                                                                                                                                                                   | N/A                                                                                                                                                                        |
| 2. (Optional.) Specify an IP address to be protected by the HTTP client verification feature. | <b>client-verify http protected</b> { <b>ip</b> <i>destination-ip-address</i>   <b>ipv6</b> <i>destination-ipv6-address</i> }<br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>port</b> <i>port-number</i> ] | By default, the HTTP client verification feature does not protect any IP address.                                                                                          |
| 3. Enter interface view.                                                                      | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                                    | N/A                                                                                                                                                                        |
| 4. Enable HTTP client verification on the interface.                                          | <b>client-verify http enable</b>                                                                                                                                                                                     | By default, HTTP client verification is disabled on the interface.<br><br>HTTP client verification can be used alone or together with an HTTP flood attack defense policy. |

## Configuring the blacklist feature

The following matrix shows the feature and hardware compatibility:

| Hardware                             | Blacklist compatibility |
|--------------------------------------|-------------------------|
| MSR954(JH296A/JH297A/ JH298A/JH299A) | No                      |
| MSR1002-4/1003-8S                    | Yes                     |
| MSR2003                              | Yes                     |
| MSR2004-24/2004-48                   | Yes                     |
| MSR3012/3024/3044/3064               | Yes                     |
| MSR4060/4080                         | Yes                     |

The blacklist feature filters packets sourced from IP addresses in blacklist entries.

Blacklist entries can be manually added or dynamically learned:

- You can manually add a blacklist entry by using the **blacklist ip** or **blacklist ipv6** command. These entries do not age out by default. You can configure an aging time for each entry.
- The device can automatically add blacklist entries when collaborating with the scanning attack detection feature. Each dynamically learned blacklist entry has an aging time, which is user configurable. Make sure the **block-source** keyword is specified as the scanning attack prevention action for collaboration. For more information about the scanning attack detection and prevention feature, see "[Configuring a scanning attack defense policy](#)."

To configure the blacklist feature:

| Step                                                     | Command                                                                                                                                                                                          | Remarks                                                                                                                                                  |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                    | <b>system-view</b>                                                                                                                                                                               | N/A                                                                                                                                                      |
| 2. (Optional.) Enable the global blacklist feature.      | <b>blacklist global enable</b>                                                                                                                                                                   | By default, the global blacklist feature is disabled.<br>If the global blacklist feature is enabled, the blacklist feature is enabled on all interfaces. |
| 3. Enter interface view.                                 | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                | N/A                                                                                                                                                      |
| 4. Enable the blacklist feature on the interface.        | <b>blacklist enable</b>                                                                                                                                                                          | By default, the blacklist feature is disabled on the interface.                                                                                          |
| 5. (Optional.) Add an IPv4 blacklist entry.              | <b>blacklist ip</b> <i>source-ip-address</i><br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ]<br>[ <b>timeout</b> <i>minutes</i> ]                                                            | By default, no IPv4 blacklist entry exists.                                                                                                              |
| 6. (Optional.) Add an IPv6 blacklist entry.              | <b>blacklist ipv6</b> <i>source-ipv6-address</i><br>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ]<br>[ <b>ds-lite-peer</b> <i>ds-lite-peer-address</i> ]<br>[ <b>timeout</b> <i>minutes</i> ] | By default, no IPv6 blacklist entry exists.                                                                                                              |
| 7. (Optional.) Enable logging for the blacklist feature. | <b>blacklist logging enable</b>                                                                                                                                                                  | By default, logging is disabled for the blacklist feature.                                                                                               |

## Displaying and maintaining attack detection and prevention

Use the **display** commands in any view and the **reset** commands in user view.

To display and maintain attack detection and prevention:

| Task                                                                                                                                         | Command                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display attack detection and prevention statistics on an interface (centralized devices in standalone mode).                                 | <b>display attack-defense statistics interface</b><br><i>interface-type interface-number</i>                                                                                                             |
| Display attack detection and prevention statistics on an interface (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display attack-defense statistics interface</b><br><i>interface-type interface-number [ slot slot-number ]</i>                                                                                        |
| Display attack detection and prevention statistics on an interface (distributed devices in IRF mode).                                        | <b>display attack-defense statistics interface</b><br><i>interface-type interface-number [ chassis chassis-number slot slot-number ]</i>                                                                 |
| Display attack detection and prevention statistics for the device (centralized devices in standalone mode).                                  | <b>display attack-defense statistics local</b>                                                                                                                                                           |
| Display attack detection and prevention statistics for the device (distributed devices in standalone mode/centralized devices in IRF mode).  | <b>display attack-defense statistics local [ slot slot-number ]</b>                                                                                                                                      |
| Display attack detection and prevention statistics for the device (distributed devices in IRF mode).                                         | <b>display attack-defense statistics local [ chassis chassis-number slot slot-number ]</b>                                                                                                               |
| Display attack defense policy configuration.                                                                                                 | <b>display attack-defense policy [ policy-name ]</b>                                                                                                                                                     |
| Display information about IPv4 scanning attackers (centralized devices in standalone mode).                                                  | <b>display attack-defense scan attacker ip [ interface interface-type interface-number   local ] [ count ]</b>                                                                                           |
| Display information about IPv4 scanning attackers (distributed devices in standalone mode/centralized devices in IRF mode).                  | <b>display attack-defense scan attacker ip [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]</b>                                                 |
| Display information about IPv4 scanning attackers (distributed devices in IRF mode).                                                         | <b>display attack-defense scan attacker ip [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ]</b>   |
| Display information about IPv6 scanning attackers (centralized devices in standalone mode).                                                  | <b>display attack-defense scan attacker ipv6 [ interface interface-type interface-number   local ] [ count ]</b>                                                                                         |
| Display information about IPv6 scanning attackers (distributed devices in standalone mode/centralized devices in IRF mode).                  | <b>display attack-defense scan attacker ipv6 [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]</b>                                               |
| Display information about IPv6 scanning attackers (distributed devices in IRF mode).                                                         | <b>display attack-defense scan attacker ipv6 [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ]</b> |
| Display information about IPv4 scanning attack victims (centralized devices in standalone mode).                                             | <b>display attack-defense scan victim ip [ interface interface-type interface-number   local ] [ count ]</b>                                                                                             |
| Display information about IPv4 scanning attack victims (distributed devices in standalone mode/centralized devices in IRF mode).             | <b>display attack-defense scan victim ip [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]</b>                                                   |
| Display information about IPv4 scanning attack victims (distributed devices in IRF mode).                                                    | <b>display attack-defense scan victim ip [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ]</b>     |
| Display information about IPv6 scanning attack victims (centralized devices in standalone mode).                                             | <b>display attack-defense scan victim ipv6 [ interface interface-type interface-number   local ] [ count ]</b>                                                                                           |

| Task                                                                                                                                                                  | Command                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display information about IPv6 scanning attack victims (distributed devices in standalone mode/centralized devices in IRF mode).                                      | <b>display attack-defense scan victim ipv6</b> [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]                                                                                                                                                                                                                       |
| Display information about IPv6 scanning attack victims (distributed devices in IRF mode).                                                                             | <b>display attack-defense scan victim ipv6</b> [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ]                                                                                                                                                                         |
| Display flood attack detection and prevention statistics for an IPv4 address (centralized devices in standalone mode).                                                | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmp-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ip [ ip-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number   local ] [ count ]                                                                                               |
| Display flood attack detection and prevention statistics for an IPv4 address (distributed devices in standalone mode/centralized devices in IRF mode).                | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmp-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ip [ ip-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]                                                     |
| Display flood attack detection and prevention statistics for an IPv4 address (distributed devices in IRF mode).                                                       | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmp-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ip [ ip-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ]       |
| Display flood attack detection and prevention statistics for an IPv6 address (centralized devices in standalone mode).                                                | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmpv6-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ipv6 [ ipv6-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number   local ] [ count ]                                                                                         |
| Display flood attack detection and prevention statistics for an IPv6 address (distributed devices in standalone mode/centralized devices in IRF mode).                | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmpv6-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ipv6 [ ipv6-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number [ slot slot-number ]   local [ slot slot-number ] ] [ count ]                                               |
| Display flood attack detection and prevention statistics for an IPv6 address (distributed devices in IRF mode).                                                       | <b>display attack-defense</b> { ack-flood   dns-flood   fin-flood   flood   http-flood   icmpv6-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } statistics ipv6 [ ipv6-address [ vpn vpn-instance-name ] ] [ interface interface-type interface-number [ chassis chassis-number slot slot-number ]   local [ chassis chassis-number slot slot-number ] ] [ count ] |
| Display information about IPv4 addresses protected by flood attack detection and prevention (centralized devices in standalone mode).                                 | <b>display attack-defense policy</b> policy-name { ack-flood   dns-flood   fin-flood   flood   http-flood   icmp-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } ip [ ip-address [ vpn vpn-instance-name ] ] [ count ]                                                                                                                                             |
| Display information about IPv4 addresses protected by flood attack detection and prevention (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display attack-defense policy</b> policy-name { ack-flood   dns-flood   fin-flood   flood   http-flood   icmp-flood   rst-flood   syn-ack-flood   syn-flood   udp-flood } ip [ ip-address [ vpn vpn-instance-name ] ] [ slot slot-number ] [ count ]                                                                                                                        |

| Task                                                                                                                                                                  | Command                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display information about IPv4 addresses protected by flood attack detection and prevention (distributed devices in IRF mode).                                        | <b>display attack-defense policy</b> <i>policy-name</i> { <b>ack-flood</b>   <b>dns-flood</b>   <b>fin-flood</b>   <b>flood</b>   <b>http-flood</b>   <b>icmp-flood</b>   <b>rst-flood</b>   <b>syn-ack-flood</b>   <b>syn-flood</b>   <b>udp-flood</b> } <b>ip</b> [ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]       |
| Display information about IPv6 addresses protected by flood attack detection and prevention (centralized devices in standalone mode).                                 | <b>display attack-defense policy</b> <i>policy-name</i> { <b>ack-flood</b>   <b>dns-flood</b>   <b>fin-flood</b>   <b>flood</b>   <b>http-flood</b>   <b>icmpv6-flood</b>   <b>rst-flood</b>   <b>syn-ack-flood</b>   <b>syn-flood</b>   <b>udp-flood</b> } <b>ipv6</b> [ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>count</b> ]                                                                         |
| Display information about IPv6 addresses protected by flood attack detection and prevention (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display attack-defense policy</b> <i>policy-name</i> { <b>ack-flood</b>   <b>dns-flood</b>   <b>fin-flood</b>   <b>flood</b>   <b>http-flood</b>   <b>icmpv6-flood</b>   <b>rst-flood</b>   <b>syn-ack-flood</b>   <b>syn-flood</b>   <b>udp-flood</b> } <b>ipv6</b> [ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                      |
| Display information about IPv6 addresses protected by flood attack detection and prevention (distributed devices in IRF mode).                                        | <b>display attack-defense policy</b> <i>policy-name</i> { <b>ack-flood</b>   <b>dns-flood</b>   <b>fin-flood</b>   <b>flood</b>   <b>http-flood</b>   <b>icmpv6-flood</b>   <b>rst-flood</b>   <b>syn-ack-flood</b>   <b>syn-flood</b>   <b>udp-flood</b> } <b>ipv6</b> [ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ] |
| Display IPv4 blacklist entries (centralized devices in standalone mode).                                                                                              | <b>display blacklist ip</b> [ <i>source-ip-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>count</b> ]                                                                                                                                                                                                                                                                                                       |
| Display IPv4 blacklist entries (distributed devices in standalone mode/centralized devices in IRF mode).                                                              | <b>display blacklist ip</b> [ <i>source-ip-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                                                                    |
| Display IPv4 blacklist entries (distributed devices in IRF mode).                                                                                                     | <b>display blacklist ip</b> [ <i>source-ip-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                               |
| Display IPv6 blacklist entries (centralized devices in standalone mode).                                                                                              | <b>display blacklist ipv6</b> [ <i>source-ipv6-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>count</b> ]                                                                                                                                                                                                                                                                                                   |
| Display IPv6 blacklist entries (distributed devices in standalone mode/centralized devices in IRF mode).                                                              | <b>display blacklist ipv6</b> [ <i>source-ipv6-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                                                                |
| Display IPv6 blacklist entries (distributed devices in IRF mode).                                                                                                     | <b>display blacklist ipv6</b> [ <i>source-ipv6-address</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                           |
| Display protected IPv4 list entries for client verification (centralized devices in standalone mode).                                                                 | <b>display client-verify</b> { <b>dns</b>   <b>http</b>   <b>tcp</b> } <b>protected ip</b> [ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b> <i>port-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                     |
| Display protected IPv4 addresses for client verification (distributed devices in standalone mode/centralized devices in IRF mode).                                    | <b>display client-verify</b> { <b>dns</b>   <b>http</b>   <b>tcp</b> } <b>protected ip</b> [ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b> <i>port-number</i> ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                                  |
| Display protected IPv4 addresses for client verification (distributed devices in IRF mode).                                                                           | <b>display client-verify</b> { <b>dns</b>   <b>http</b>   <b>tcp</b> } <b>protected ip</b> [ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b> <i>port-number</i> ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                             |
| Display protected IPv6 addresses for client verification (centralized devices in standalone mode).                                                                    | <b>display client-verify</b> { <b>dns</b>   <b>http</b>   <b>tcp</b> } <b>protected ipv6</b> [ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b> <i>port-number</i> ] [ <b>count</b> ]                                                                                                                                                                                                                 |
| Display protected IPv6 addresses for client verification (distributed devices in standalone mode/centralized devices in IRF mode).                                    | <b>display client-verify</b> { <b>dns</b>   <b>http</b>   <b>tcp</b> } <b>protected ipv6</b> [ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b> <i>port-number</i> ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                                                                                                                                                              |

| Task                                                                                                                             | Command                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display protected IPv6 addresses for client verification (distributed devices in IRF mode).                                      | <b>display client-verify { dns   http   tcp } protected ipv6</b><br>[ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>port</b><br><i>port-number</i> ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b><br><i>slot-number</i> ] [ <b>count</b> ] |
| Display trusted IPv4 addresses for client verification (centralized devices in standalone mode).                                 | <b>display client-verify { dns   http   tcp } trusted ip</b><br>[ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>count</b> ]                                                                                                                        |
| Display trusted IPv4 addresses for client verification (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display client-verify { dns   http   tcp } trusted ip</b><br>[ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>slot</b><br><i>slot-number</i> ] [ <b>count</b> ]                                                                                  |
| Display trusted IPv4 addresses for client verification (distributed devices in IRF mode).                                        | <b>display client-verify { dns   http   tcp } trusted ip</b><br>[ <i>ip-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b><br><i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                             |
| Display trusted IPv6 addresses for client verification (centralized devices in standalone mode).                                 | <b>display client-verify { dns   http   tcp } trusted ipv6</b><br>[ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>count</b> ]                                                                                                                    |
| Display trusted IPv6 addresses for client verification (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display client-verify { dns   http   tcp } trusted ipv6</b><br>[ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>slot</b><br><i>slot-number</i> ] [ <b>count</b> ]                                                                              |
| Display trusted IPv6 addresses for client verification (distributed devices in IRF mode).                                        | <b>display client-verify { dns   http   tcp } trusted ipv6</b><br>[ <i>ipv6-address</i> [ <b>vpn</b> <i>vpn-instance-name</i> ] ] [ <b>chassis</b><br><i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ]                                         |
| Clear attack detection and prevention statistics for an interface.                                                               | <b>reset attack-defense statistics interface</b><br><i>interface-type interface-number</i>                                                                                                                                                                            |
| Clear attack detection and prevention statistics for the device.                                                                 | <b>reset attack-defense statistics local</b>                                                                                                                                                                                                                          |
| Clear flood attack detection and prevention statistics.                                                                          | <b>reset attack-defense policy <i>policy-name</i> flood</b><br><b>protected { ip   ipv6 } statistics</b>                                                                                                                                                              |
| Clear dynamic IPv4 blacklist entries.                                                                                            | <b>reset blacklist ip { <i>source-ip-address</i> [ <b>vpn-instance</b><br/><i>vpn-instance-name</i> ] [ <b>ds-lite-peer</b><br/><i>ds-lite-peer-address</i> ]   all }</b>                                                                                             |
| Clear dynamic IPv6 blacklist entries.                                                                                            | <b>reset blacklist ipv6 { <i>source-ipv6-address</i><br/>[ <b>vpn-instance</b> <i>vpn-instance-name</i> ]   all }</b>                                                                                                                                                 |
| Clear blacklist statistics.                                                                                                      | <b>reset blacklist statistics</b>                                                                                                                                                                                                                                     |
| Clear protected IP statistics for client verification.                                                                           | <b>reset client-verify { dns   http   tcp } protected { ip  <br/>ipv6 } statistics</b>                                                                                                                                                                                |
| Clear the trusted IP list for client verification.                                                                               | <b>reset client-verify { dns   http   tcp } trusted { ip  <br/>ipv6 }</b>                                                                                                                                                                                             |



# Attack detection and prevention configuration examples

## Interface-based attack detection and prevention configuration example

### Network requirements

As shown in [Figure 154](#), Router is the gateway for the internal network. GigabitEthernet 2/0/2 connects to the external network, and GigabitEthernet 2/0/3 connects to an internal server.

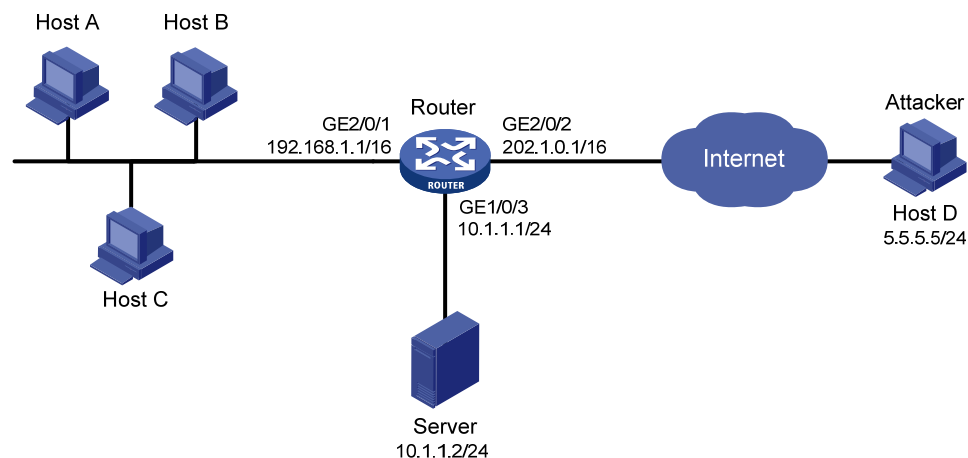
To protect the internal hosts and internal server against scanning attacks and smurf attacks, configure an attack defense policy to meet the following requirements:

- Configure low-level scanning attack detection. Configure the device to log scanning attacks and keep the attackers' IP addresses on the blacklist for 10 minutes.
- Configure signature detection for smurf attack, and configure the device to log smurf attacks.

To protect the internal server against SYN flood attacks, configure another attack defense policy to meet the following requirements:

- Set the attack prevention triggering threshold to 5000 packets per second.
- Specify the prevention action as packet dropping and logging.

**Figure 154 Network diagram**



### Configuration procedure

# Configure IP addresses for the interfaces on Router. (Details not shown.)

# Enable the global blacklist feature.

```
<Router> system-view
```

```
[Router] blacklist global enable
```

# Create attack defense policy **a1**.

```
[Router] attack-defense policy a1
```

# Configure signature detection for smurf attacks, and specify the prevention action as **logging**.

```
[Router-attack-defense-policy-a1] signature detect smurf action logging
```

# Configure low level scanning attack detection. Specify the prevention action as **logging** and **block-source**, and set the aging time to 10 minutes for the blacklist entries.

```
[Router-attack-defense-policy-a1] scan detect level low action logging block-source
timeout 10

Configure SYN flood attack detection for 10.1.1.2. Set the threshold for triggering attack prevention
to 5000. Specify the prevention actions as logging and drop.
[Router-attack-defense-policy-a1] syn-flood detect ip 10.1.1.2 threshold 5000 action
logging drop
[Router-attack-defense-policy-a1] quit

Apply attack defense policy a1 to interface GigabitEthernet 2/0/2.
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] attack-defense apply policy a1
[Router-GigabitEthernet2/0/2] quit
```

## Verifying the configuration

# Verify that the attack defense policy **a1** is successfully configured.

```
[Router] display attack-defense policy a1
Attack-defense Policy Information
```

```

Policy name : a1
Applied list : GE2/0/2

```

```
Exempt IPv4 ACL : Not configured
Exempt IPv6 ACL : Not configured

```

```
Actions: CV-Client verify BS-Block source L-Logging D-Drop N-None
```

Signature attack defense configuration:

| Signature name     | Defense        | Level         | Actions  |
|--------------------|----------------|---------------|----------|
| Fragment           | Disabled       | low           | L        |
| Impossible         | Disabled       | medium        | L,D      |
| Teardrop           | Disabled       | medium        | L,D      |
| Tiny fragment      | Disabled       | low           | L        |
| IP option abnormal | Disabled       | medium        | L,D      |
| <b>Smurf</b>       | <b>Enabled</b> | <b>medium</b> | <b>L</b> |
| Traceroute         | Disabled       | low           | L        |
| Ping of death      | Disabled       | medium        | L,D      |
| Large ICMP         | Disabled       | info          | L        |
| Max length         | 4000 bytes     |               |          |
| Large ICMPv6       | Disabled       | info          | L        |
| Max length         | 4000 bytes     |               |          |
| TCP invalid flags  | Disabled       | medium        | L,D      |
| TCP null flag      | Disabled       | medium        | L,D      |
| TCP all flags      | Disabled       | medium        | L,D      |
| TCP SYN-FIN flags  | Disabled       | medium        | L,D      |
| TCP FIN only flag  | Disabled       | medium        | L,D      |
| TCP Land           | Disabled       | medium        | L,D      |
| Winnuke            | Disabled       | medium        | L,D      |
| UDP Bomb           | Disabled       | medium        | L,D      |
| UDP Snork          | Disabled       | medium        | L,D      |
| UDP Fragggle       | Disabled       | medium        | L,D      |



|                                   |          |      |   |
|-----------------------------------|----------|------|---|
| IP option record route            | Disabled | info | L |
| IP option internet timestamp      | Disabled | info | L |
| IP option security                | Disabled | info | L |
| IP option loose source routing    | Disabled | info | L |
| IP option stream ID               | Disabled | info | L |
| IP option strict source routing   | Disabled | info | L |
| IP option route alert             | Disabled | info | L |
| ICMP echo request                 | Disabled | info | L |
| ICMP echo reply                   | Disabled | info | L |
| ICMP source quench                | Disabled | info | L |
| ICMP destination unreachable      | Disabled | info | L |
| ICMP redirect                     | Disabled | info | L |
| ICMP time exceeded                | Disabled | info | L |
| ICMP parameter problem            | Disabled | info | L |
| ICMP timestamp request            | Disabled | info | L |
| ICMP timestamp reply              | Disabled | info | L |
| ICMP information request          | Disabled | info | L |
| ICMP information reply            | Disabled | info | L |
| ICMP address mask request         | Disabled | info | L |
| ICMP address mask reply           | Disabled | info | L |
| ICMPv6 echo request               | Disabled | info | L |
| ICMPv6 echo reply                 | Disabled | info | L |
| ICMPv6 group membership query     | Disabled | info | L |
| ICMPv6 group membership report    | Disabled | info | L |
| ICMPv6 group membership reduction | Disabled | info | L |
| ICMPv6 destination unreachable    | Disabled | info | L |
| ICMPv6 time exceeded              | Disabled | info | L |
| ICMPv6 parameter problem          | Disabled | info | L |
| ICMPv6 packet too big             | Disabled | info | L |

#### Scan attack defense configuration:

Defense : Enabled

Level : low

Actions : L,BS(10)

#### Flood attack defense configuration:

| Flood type    | Global thres(pps) | Global actions | Service ports | Non-specific |
|---------------|-------------------|----------------|---------------|--------------|
| SYN flood     | 1000(default)     | -              | -             | Disabled     |
| ACK flood     | 1000(default)     | -              | -             | Disabled     |
| SYN-ACK flood | 1000(default)     | -              | -             | Disabled     |
| RST flood     | 1000(default)     | -              | -             | Disabled     |
| FIN flood     | 1000(default)     | -              | -             | Disabled     |
| UDP flood     | 1000(default)     | -              | -             | Disabled     |
| ICMP flood    | 1000(default)     | -              | -             | Disabled     |
| ICMPv6 flood  | 1000(default)     | -              | -             | Disabled     |
| DNS flood     | 1000(default)     | -              | 53            | Disabled     |
| HTTP flood    | 1000(default)     | -              | 80            | Disabled     |

Flood attack defense for protected IP addresses:

| Address  | VPN instance | Flood type | Thres(pps) | Actions | Ports |
|----------|--------------|------------|------------|---------|-------|
| 10.1.1.2 | --           | SYN-FLOOD  | 5000       | L,D     | -     |

# Verify that the attack detection and prevention takes effect on GigabitEthernet 2/0/2.

[Router] display attack-defense statistics interface gigabitethernet 2/0/2

Attack policy name: a1

Scan attack defense statistics:

| AttackType           | AttackTimes | Dropped |
|----------------------|-------------|---------|
| Port scan            | 2           | 0       |
| IP sweep             | 3           | 0       |
| Distribute port scan | 1           | 0       |

Flood attack defense statistics:

| AttackType | AttackTimes | Dropped |
|------------|-------------|---------|
| SYN flood  | 1           | 5000    |

Signature attack defense statistics:

| AttackType | AttackTimes | Dropped |
|------------|-------------|---------|
| Smurf      | 1           | 0       |

# Verify that the IPv4 blacklist feature collaborates with the scanning attack detection.

[Router] display blacklist ip

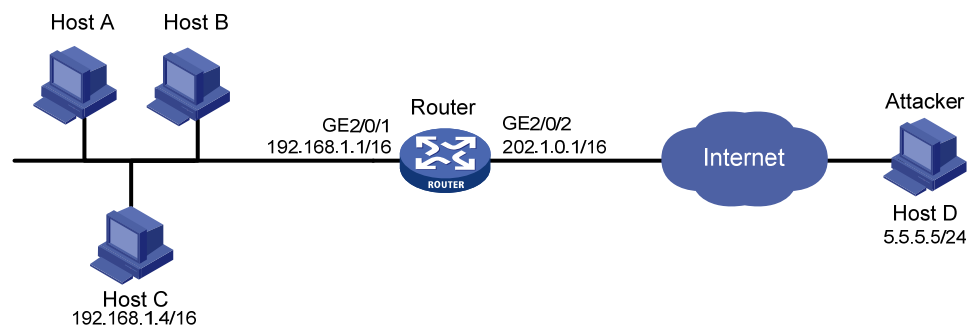
| IP address | VPN instance | DS-Lite tunnel peer | Type    | TTL(sec) | Dropped |
|------------|--------------|---------------------|---------|----------|---------|
| 5.5.5.5    | --           | --                  | Dynamic | 600      | 353452  |

## Blacklist configuration example

### Network requirements

As shown in [Figure 155](#), configure the blacklist feature on the router to block packets from the attacker Host D permanently and from Host C for 50 minutes.

**Figure 155 Network diagram**



### Configuration procedure

# Configure IP addresses for the interfaces on Router. (Details not shown.)

# Enable the global blacklist feature.

```
<Router> system-view
```

```
[Router] blacklist global enable
```

# Add a blacklist entry for Host D.

```
[Router] blacklist ip 5.5.5.5
```

# Add a blacklist entry for Host C and set the aging time to 50 minutes for the entry.

```
[Router] blacklist ip 192.168.1.4 timeout 50
```

## Verifying the configuration

# Verify that the blacklist entries are successfully added.

```
<Router> display blacklist ip
```

| IP address  | VPN instance | DS-Lite tunnel peer | Type   | TTL(sec) | Dropped |
|-------------|--------------|---------------------|--------|----------|---------|
| 5.5.5.5     | --           | --                  | Manual | Never    | 0       |
| 192.168.1.4 | --           | --                  | Manual | 2989     | 0       |

# Verify that the router drops packets from Host D. (Details not shown.)

# Execute the **undo blacklist ip 5.5.5.5** command and verify that the router forwards packets from Host D. (Details not shown.)

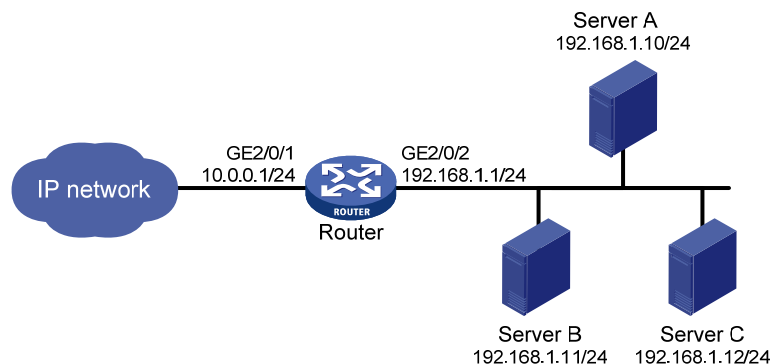
# Verify that the router drops packets from Host C for 50 minutes and forwards packets from Host C after 50 minutes. (Details not shown.)

## TCP client verification configuration example

### Network requirements

As shown in [Figure 156](#), configure TCP client verification in SYN cookie mode on Router to protect the internal servers against SYN flood attacks.

**Figure 156 Network requirements**



### Configuration procedure

# Configure IP addresses for the interfaces on Router. (Details not shown.)

# Create attack defense policy **a1**.

```
<Router> system-view
```

```
[Router] attack-defense policy a1
```

# Enable SYN flood attack detection for non-specific IP addresses.

```
[Router-attack-defense-policy-a1] syn-flood detect non-specific
```

# Set the global threshold to 10000 for triggering SYN flood attack prevention.

```
[Router-attack-defense-policy-a1] syn-flood threshold 10000
```

# Specify **logging** and **client-verify** as the global actions against SYN flood attacks.

```
[Router-attack-defense-policy-a1] syn-flood action logging client-verify
```

```
[Router-attack-defense-policy-a1] quit
```

# Apply attack defense policy **a1** to interface GigabitEthernet 2/0/1.

```
[Router] interface gigabitethernet 2/0/1
```

```
[Router-GigabitEthernet2/0/1] attack-defense apply policy a1
```

```
[Router-GigabitEthernet2/0/1] quit
Enable TCP client verification in SYN cookie mode on interface GigabitEthernet 2/0/1.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] client-verify tcp enable mode syn-cookie
[Router-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

# If a SYN flood attack occurs, verify that the victim's IP address is added to the protected IP list for TCP client verification.

```
[Router] display client-verify tcp protected ip
```

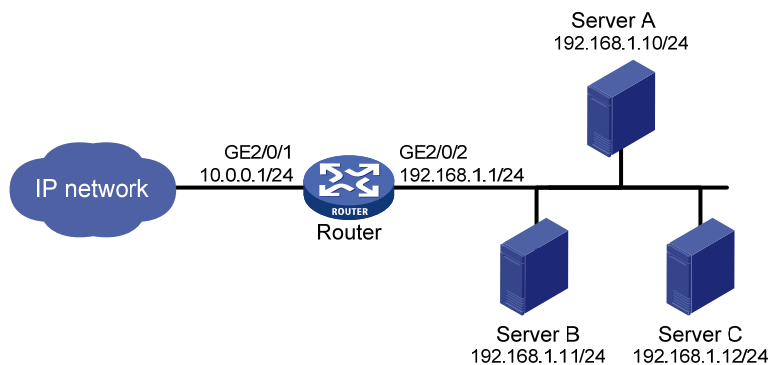
| IP address   | VPN instance | Port | Type    | Requested | Trusted |
|--------------|--------------|------|---------|-----------|---------|
| 192.168.1.10 | --           | any  | Dynamic | 20        | 12      |

# DNS client verification configuration example

## Network requirements

As shown in [Figure 157](#), configure DNS client verification on Router to protect internal servers against DNS flood attacks.

**Figure 157 Network diagram**



## Configuration procedure

```
Configure IP addresses for the interfaces on Router. (Details not shown.)
Create attack defense policy a1.
<Router> system-view
[Router] attack-defense policy a1
Enable DNS flood attack detection for non-specific IP addresses.
[Router-attack-defense-policy-a1] dns-flood detect non-specific
Set the global threshold to 10000 for triggering DNS flood attack prevention.
[Router-attack-defense-policy-a1] dns-flood threshold 10000
Specify logging and client-verify as the global actions against DNS flood attacks.
[Router-attack-defense-policy-a1] dns-flood action logging client-verify
[Router-attack-defense-policy-a1] quit
Apply attack defense policy a1 to interface GigabitEthernet 2/0/1.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] attack-defense apply policy a1
[Router-GigabitEthernet2/0/1] quit
```

```
Enable DNS client verification on interface GigabitEthernet 2/0/1.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] client-verify dns enable
[Router-GigabitEthernet2/0/1] quit
```

### Verifying the configuration

# If a DNS flood attack occurs, verify that the victim's IP address is added to the protected IP list for DNS client verification.

```
[Router] display client-verify dns protected ip
```

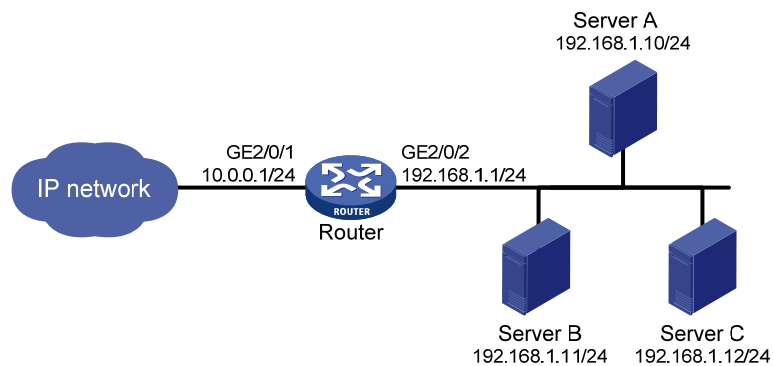
| IP address   | VPN instance | Port | Type    | Requested | Trusted |
|--------------|--------------|------|---------|-----------|---------|
| 192.168.1.10 | --           | 53   | Dynamic | 20        | 12      |

## HTTP client verification configuration example

### Network requirements

As shown in [Figure 158](#), configure HTTP client verification on Router to protect internal servers against HTTP flood attacks.

**Figure 158 Network diagram**



### Configuration procedure

```
Configure IP addresses for the interfaces on Router. (Details not shown.)
Create attack defense policy a1.
<Router> system-view
[Router] attack-defense policy a1

Enable HTTP flood attack detection for non-specific IP addresses.
[Router-attack-defense-policy-a1] http-flood detect non-specific

Set the global threshold to 10000 for triggering HTTP flood attack prevention.
[Router-attack-defense-policy-a1] http-flood threshold 10000

Specify logging and client-verify as the global actions against HTTP flood attacks.
[Router-attack-defense-policy-a1] http-flood action logging client-verify
[Router-attack-defense-policy-a1] quit

Apply attack defense policy a1 to interface GigabitEthernet 2/0/1.
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] attack-defense apply policy a1
[Router-GigabitEthernet2/0/1] quit

Enable HTTP client verification on interface GigabitEthernet 2/0/1.
```

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] client-verify http enable
[Router-GigabitEthernet2/0/1] quit
```

### Verifying the configuration

# If an HTTP flood attack occurs, verify that the victim's IP address is added to the protected IP list for HTTP client verification.

```
[Router] display client-verify http protected ip
```

| IP address   | VPN instance | Port | Type    | Requested | Trusted |
|--------------|--------------|------|---------|-----------|---------|
| 192.168.1.10 | --           | 8080 | Dynamic | 20        | 12      |

# Configuring IP source guard

## Overview

IP source guard (IPSG) prevents spoofing attacks by using an IPSG binding table to match legitimate packets. It drops packets that do not match the table. IPSG is a per-interface packet filter. Configuring the feature on one interface does not affect packet forwarding on another interface.

The IPSG bindings are interface-specific. The bindings fall into the following types:

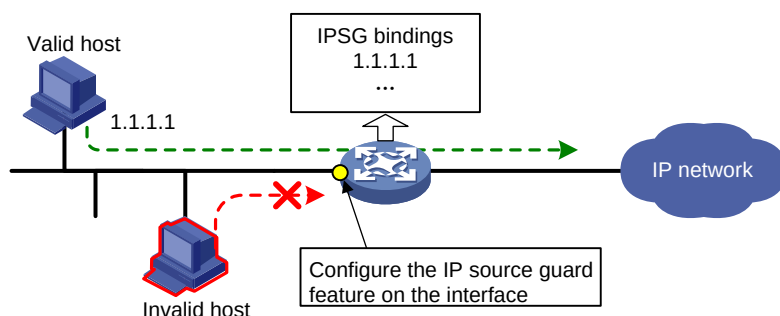
- IP.
- MAC.
- IP-MAC.
- IP-VLAN.
- MAC-VLAN.
- IP-MAC-VLAN.

IPSG bindings can be static or dynamic.

- **Static bindings**—Configured manually.
- **Dynamic bindings**—Generated based on information from other modules. For more information about dynamic bindings, see "[Dynamic IPSG bindings](#)."

As shown in [Figure 159](#), IPSG forwards only the packets that match an IPSG binding.

**Figure 159 Diagram for the IPSG feature**



## Static IPSG bindings

Static IPSG bindings are configured manually. They are suitable for scenarios where few hosts exist on a LAN and their IP addresses are manually configured. For example, you can configure a static IPSG binding on an interface that connects to a server. This binding allows the interface to receive packets only from the server.

Static IPSG bindings on an interface filter incoming IPv4 or IPv6 packets on the interface.

A static IPSG binding binds the IP address, MAC address, VLAN, or any combination of the items in interface view. The binding takes effect only on the interface to check the validity of users who are attempting to access the interface.

## Dynamic IPSG bindings

IPSG automatically obtains user information from other modules to generate dynamic bindings. The source modules include 802.1X, DHCP relay, DHCP snooping, DHCPv6 snooping, and DHCP server.

DHCP-based IPSG bindings are suitable for scenarios where hosts on a LAN obtain IP addresses through DHCP. IPSG is configured on the DHCP snooping device or the DHCP relay agent. It generates dynamic bindings based on the DHCP snooping entries or DHCP relay entries. IPSG allows only packets from the DHCP clients to pass through.

### Dynamic IPv4SG

Dynamic bindings generated based on different source modules are for different usages:

| Interface types       | Source modules   | Binding usage                                              |
|-----------------------|------------------|------------------------------------------------------------|
| Layer 2 Ethernet port | DHCP snooping    | Packet filtering.                                          |
|                       | 802.1X           | For cooperation with modules to provide security services. |
| VLAN interface        | DHCP relay agent | Packet filtering.                                          |
|                       | DHCP server      | For cooperation with modules to provide security services. |

For more information about 802.1X, see "[Configuring 802.1X](#)." For information about DHCP snooping, DHCP relay, and DHCP server see *Layer 3—IP Services Configuration Guide*.

### Dynamic IPv6SG

IPv6SG on an interface obtains information from DHCPv6 snooping entries to generate bindings for packet filtering.

For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.

## IPSG configuration task list

To configure IPv4SG, perform the following tasks:

| Tasks at a glance                                               |
|-----------------------------------------------------------------|
| (Required.) <a href="#">Enabling IPv4SG on an interface</a>     |
| (Optional.) <a href="#">Configuring a static IPv4SG binding</a> |

To configure IPv6SG, perform the following tasks:

| Tasks at a glance                                               |
|-----------------------------------------------------------------|
| (Required.) <a href="#">Enabling IPv6SG on an interface</a>     |
| (Optional.) <a href="#">Configuring a static IPv6SG binding</a> |

## Configuring the IPv4SG feature

You cannot configure the IPv4SG feature on a service loopback interface. If IPv4SG is enabled on an interface, you cannot assign the interface to a service loopback group.



## Enabling IPv4SG on an interface

When you enable IPSG on an interface, the static and dynamic IPSG are both enabled.

- Static IPv4SG uses static bindings configured by using the **ip source binding** command.
- Dynamic IPv4SG generates dynamic bindings from related source modules. IPv4SG uses the bindings to filter incoming IPv4 packets based on the matching criteria specified in the **ip verify source** command.

To implement dynamic IPv4SG, make sure the DHCP snooping or DHCP relay feature operates correctly on the network.

To enable the IPv4SG feature on an interface:

| Step                          | Command                                                                                                            | Remarks                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.         | <b>system-view</b>                                                                                                 | N/A                                                                                                                                                                          |
| 2. Enter interface view.      | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                  | The following interface types are supported: <ul style="list-style-type: none"><li>• Layer 2 Ethernet port.</li><li>• VLAN interface.</li></ul>                              |
| 3. Enable the IPv4SG feature. | <b>ip verify source</b><br>{ <b>ip-address</b>   <b>ip-address</b><br><b>mac-address</b>  <br><b>mac-address</b> } | By default, the IPv4SG feature is disabled on an interface.<br><br>If you configure this command on an interface multiple times, the most recent configuration takes effect. |

## Configuring a static IPv4SG binding

| Step                                  | Command                                                                                                                                                                                                                         | Remarks                                                                                                                                                                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                 | <b>system-view</b>                                                                                                                                                                                                              | N/A                                                                                                                                                                                                                                                     |
| 2. Enter interface view.              | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                                               | The following interface types are supported: <ul style="list-style-type: none"><li>• Layer 2 Ethernet port.</li><li>• VLAN interface.</li></ul>                                                                                                         |
| 3. Configure a static IPv4SG binding. | <b>ip source binding</b> { <b>ip-address</b><br><i>ip-address</i>   <b>ip-address</b><br><i>ip-address</i> <b>mac-address</b><br><i>mac-address</i>   <b>mac-address</b><br><i>mac-address</i> } [ <b>vlan</b> <i>vlan-id</i> ] | By default, no static IPv4SG binding is configured on an interface.<br><br>The <b>vlan</b> <i>vlan-id</i> option is supported only in Layer 2 Ethernet interface view.<br><br>You can configure the same static IPv4SG binding on different interfaces. |

## Configuring the IPv6SG feature

You cannot configure the IPv6SG feature on a service loopback interface. If IPv6SG is enabled on an interface, you cannot assign the interface to a service loopback group.

## Enabling IPv6SG on an interface

When you enable IPv6SG on an interface, the static and dynamic IPv6SG are both enabled.

- Static IPv6SG uses static bindings configured by using the **ipv6 source binding** command.

- Dynamic IPv6SG generates dynamic bindings from related source modules. IPv6SG uses the bindings to filter incoming IPv6 packets based on the matching criteria specified in the **ipv6 verify source** command.

To implement dynamic IPv6SG, make sure DHCPv6 snooping operates correctly on the network.

To enable the IPv6SG feature on an interface:

| Step                          | Command                                                                                                           | Remarks                                                                                                                                                                  |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.         | <b>system-view</b>                                                                                                | N/A                                                                                                                                                                      |
| 2. Enter interface view.      | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                 | The following interface types are supported: <ul style="list-style-type: none"> <li>Layer 2 Ethernet port.</li> <li>VLAN interface.</li> </ul>                           |
| 3. Enable the IPv6SG feature. | <b>ipv6 verify source</b><br>{ <b>ip-address</b>   <b>ip-address</b><br><b>mac-address</b>   <b>mac-address</b> } | By default, the IPv6SG feature is disabled on an interface.<br>If you configure this command on an interface multiple times, the most recent configuration takes effect. |

## Configuring a static IPv6SG binding

| Step                                  | Command                                                                                                                                                                                                                                  | Remarks                                                                                                                                                                                                                                         |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                 | <b>system-view</b>                                                                                                                                                                                                                       | N/A                                                                                                                                                                                                                                             |
| 2. Enter interface view.              | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                                                        | The following interface types are supported: <ul style="list-style-type: none"> <li>Layer 2 Ethernet port.</li> <li>VLAN interface.</li> </ul>                                                                                                  |
| 3. Configure a static IPv6SG binding. | <b>ipv6 source binding</b><br>{ <b>ip-address</b> <i>ipv6-address</i>  <br><b>ip-address</b> <i>ipv6-address</i><br><b>mac-address</b> <i>mac-address</i>  <br><b>mac-address</b> <i>mac-address</i> }<br>[ <b>vlan</b> <i>vlan-id</i> ] | By default, no static IPv6SG binding is configured on an interface.<br>The <b>vlan</b> <i>vlan-id</i> option is supported only in Layer 2 Ethernet interface view.<br>You can configure the same static IPv6SG binding on different interfaces. |

## Displaying and maintaining IPSG

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                                                              | Command                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display IPv4SG bindings (centralized devices in standalone mode).                                 | <b>display ip source binding</b> [ <b>static</b>   [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>dhcp-relay</b>   <b>dhcp-server</b>   <b>dhcp-snooping</b>   <b>dot1x</b> ] ] [ <b>ip-address</b> <i>ip-address</i> ] [ <b>mac-address</b> <i>mac-address</i> ] [ <b>vlan</b> <i>vlan-id</i> ] [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]                                    |
| Display IPv4SG bindings (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display ip source binding</b> [ <b>static</b>   [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] [ <b>dhcp-relay</b>   <b>dhcp-server</b>   <b>dhcp-snooping</b>   <b>dot1x</b> ] ] [ <b>ip-address</b> <i>ip-address</i> ] [ <b>mac-address</b> <i>mac-address</i> ] [ <b>vlan</b> <i>vlan-id</i> ] [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ] [ <b>slot</b> <i>slot-number</i> ] |
| Display IPv4SG bindings                                                                           | <b>display ip source binding</b> [ <b>static</b>   [ <b>vpn-instance</b>                                                                                                                                                                                                                                                                                                                                      |

| Task                                                                                              | Command                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (distributed devices in IRF mode).                                                                | <code>vpn-instance-name</code> [ <code>dhcp-relay</code>   <code>dhcp-server</code>   <code>dhcp-snooping</code>   <code>dot1x</code> ] [ <code>ip-address</code> <i>ip-address</i> ] [ <code>mac-address</code> <i>mac-address</i> ] [ <code>vlan</code> <i>vlan-id</i> ] [ <code>interface</code> <i>interface-type interface-number</i> ] [ <code>chassis</code> <i>chassis-number slot slot-number</i> ]                      |
| Display IPv6SG bindings (centralized devices in standalone mode).                                 | <code>display ipv6 source binding</code> [ <code>static</code>   [ <code>vpn-instance</code> <i>vpn-instance-name</i> ] [ <code>dhcpv6-snooping</code> ] ] [ <code>ip-address</code> <i>ipv6-address</i> ] [ <code>mac-address</code> <i>mac-address</i> ] [ <code>vlan</code> <i>vlan-id</i> ] [ <code>interface</code> <i>interface-type interface-number</i> ]                                                                 |
| Display IPv6SG bindings (distributed devices in standalone mode/centralized devices in IRF mode). | <code>display ipv6 source binding</code> [ <code>static</code>   [ <code>vpn-instance</code> <i>vpn-instance-name</i> ] [ <code>dhcpv6-snooping</code> ] ] [ <code>ip-address</code> <i>ipv6-address</i> ] [ <code>mac-address</code> <i>mac-address</i> ] [ <code>vlan</code> <i>vlan-id</i> ] [ <code>interface</code> <i>interface-type interface-number</i> ] [ <code>slot</code> <i>slot-number</i> ]                        |
| Display IPv6 bindings (distributed devices in IRF mode).                                          | <code>display ipv6 source binding</code> [ <code>static</code>   [ <code>vpn-instance</code> <i>vpn-instance-name</i> ] [ <code>dhcpv6-snooping</code> ] ] [ <code>ip-address</code> <i>ipv6-address</i> ] [ <code>mac-address</code> <i>mac-address</i> ] [ <code>vlan</code> <i>vlan-id</i> ] [ <code>interface</code> <i>interface-type interface-number</i> ] [ <code>chassis</code> <i>chassis-number slot slot-number</i> ] |

# IPSG configuration examples

## Static IPv4SG configuration example

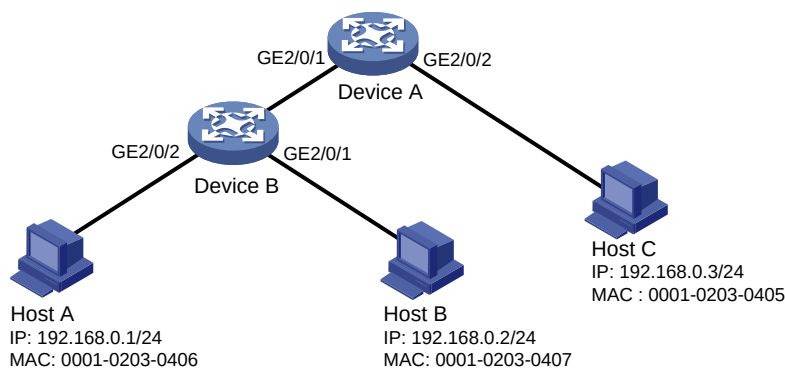
### Network requirements

As shown in [Figure 160](#), all hosts use static IP addresses.

Configure static IPv4SG bindings on Device A and Device B to meet the following requirements:

- GigabitEthernet 2/0/2 of Device A allows only IP packets from Host C to pass.
- GigabitEthernet 2/0/1 of Device A allows only IP packets from Host A to pass.
- GigabitEthernet 2/0/1 of Device B allows IP packets from Host B to pass.

**Figure 160 Network diagram**



### Configuration procedure

1. Configure Device A:  
 # Configure IP addresses for the interfaces. (Details not shown.)  
 # Enable IPv4SG on GigabitEthernet 2/0/2.  
 <DeviceA> system-view  
 [DeviceA] interface gigabitethernet 2/0/2

```

[DeviceA-GigabitEthernet2/0/2] ip verify source ip-address mac-address
On GigabitEthernet 2/0/2, configure a static IPv4SG binding for Host C.
[DeviceA-GigabitEthernet2/0/2] ip source binding ip-address 192.168.0.3 mac-address
0001-0203-0405
[DeviceA-GigabitEthernet2/0/2] quit
Enable IPv4SG on GigabitEthernet 2/0/1.
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip verify source ip-address mac-address
On GigabitEthernet 2/0/1, configure a static IPv4SG binding for Host A.
[DeviceA-GigabitEthernet2/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[DeviceA-GigabitEthernet2/0/1] quit
2. Configure Device B:
Configure an IP address for each interface. (Details not shown.)
Enable IPv4SG on GigabitEthernet 2/0/2.
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet2/0/2] quit
Enable IPv4SG on GigabitEthernet 2/0/1.
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip verify source ip-address mac-address
On GigabitEthernet 2/0/1, configure a static IPv4SG binding for Host B.
[DeviceB-GigabitEthernet2/0/1] ip source binding mac-address 0001-0203-0407
[DeviceB-GigabitEthernet2/0/1] quit

```

## Verifying the configuration

# Verify that the static IPv4SG bindings are configured successfully on Device A.

```
<DeviceA> display ip source binding static
```

Total entries found: 2

| IP Address  | MAC Address    | Interface | VLAN | Type   |
|-------------|----------------|-----------|------|--------|
| 192.168.0.1 | 0001-0203-0405 | GE2/0/2   | N/A  | Static |
| 192.168.0.3 | 0001-0203-0406 | GE2/0/1   | N/A  | Static |

# Verify that the static IPv4SG bindings are configured successfully on Device B.

```
<DeviceB> display ip source binding static
```

Total entries found: 2

| IP Address | MAC Address    | Interface | VLAN | Type   |
|------------|----------------|-----------|------|--------|
| N/A        | 0001-0203-0407 | GE2/0/1   | N/A  | Static |

## Dynamic IPv4SG using DHCP snooping configuration example

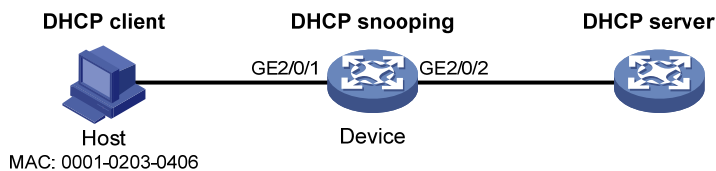
### Network requirements

As shown in [Figure 161](#), the host (the DHCP client) obtains an IP address from the DHCP server.

Enable DHCP snooping on the device to record the IPv4 address and the MAC address of the host in a DHCP snooping entry.

Enable dynamic IPv4SG on GigabitEthernet 2/0/1 to filter received packets based on DHCP snooping entries. Only packets from the client that obtains an IP address from the DHCP server are allowed to pass.

**Figure 161 Network diagram**



## Configuration procedure

1. Configure the DHCP server.  
For information about DHCP server configuration, see *Layer 3—IP Services Configuration Guide*.
2. Configure the device:
  - # Configure IP addresses for the interfaces. (Details not shown.)
  - # Enable DHCP snooping.
  - <Device> system-view
  - [Device] dhcp snooping enable
  - # Configure GigabitEthernet 2/0/2 as a trusted interface.
  - [Device] interface gigabitethernet 2/0/2
  - [Device-GigabitEthernet2/0/2] dhcp snooping trust
  - [Device-GigabitEthernet2/0/2] quit
  - # Enable IPv4SG on GigabitEthernet 2/0/1 and verify the source IP address and MAC address for dynamic IPSG.
  - [Device] interface gigabitethernet 2/0/1
  - [Device-GigabitEthernet2/0/1] ip verify source ip-address mac-address
  - # Enable recording of client information in DHCP snooping entries on GigabitEthernet 2/0/1.
  - [Device-GigabitEthernet2/0/1] dhcp snooping binding record
  - [Device-GigabitEthernet2/0/1] quit

## Verifying the configuration

# Verify that a dynamic IPv4SG binding is generated based on a DHCP snooping entry.

```
[Device] display ip source binding dhcp-snooping
```

Total entries found: 1

| IP Address  | MAC Address    | Interface | VLAN | Type          |
|-------------|----------------|-----------|------|---------------|
| 192.168.0.1 | 0001-0203-0406 | GE2/0/1   | 1    | DHCP snooping |

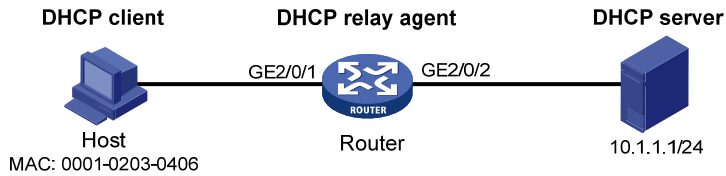
## Dynamic IPv4SG using DHCP relay configuration example

### Network requirements

As shown in [Figure 162](#), DHCP relay is enabled on the router. The host obtains an IP address from the DHCP server through the DHCP relay agent.

Enable dynamic IPv4SG on interface GigabitEthernet 2/0/1 to filter received packets based on the DHCP relay entry.

**Figure 162 Network diagram**



## Configuration procedure

1. Configure the DHCP relay agent:
  - # Configure IP addresses for the interfaces. (Details not shown.)
  - # Enable the DHCP service.

```
<Router> system-view
[Router] dhcp enable
```
  - # Enable recording DHCP relay client entries.

```
[Router] dhcp relay client-information record
```
  - # Configure interface GigabitEthernet 2/0/1 to operate in DHCP relay mode.

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] dhcp select relay
```
  - # Specify the IP address of the DHCP server.

```
[Router-GigabitEthernet2/0/1] dhcp relay server-address 10.1.1.1
[Router-GigabitEthernet2/0/1] quit
```
2. Enable IPv4SG on interface GigabitEthernet 2/0/1 and verify the source IP address and MAC address for dynamic IPSG.

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] ip verify source ip-address mac-address
[Router-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

```
Verify that a dynamic IPv4SG binding is generated based on a DHCP relay entry.
[Router] display ip source binding dhcp-relay
Total entries found: 1
```

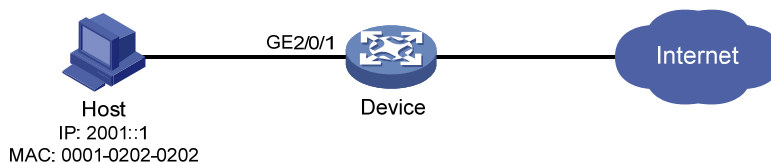
| IP Address  | MAC Address    | Interface | VLAN | Type       |
|-------------|----------------|-----------|------|------------|
| 192.168.0.1 | 0001-0203-0406 | GE2/0/1   | N/A  | DHCP relay |

## Static IPv6SG configuration example

### Network requirements

As shown in [Figure 163](#), configure a static IPv6SG binding on GigabitEthernet 2/0/1 of the device to allow only IPv6 packets from the host to pass.

**Figure 163 Network diagram**



## Configuration procedure

```
Enable IPv6SG on GigabitEthernet 2/0/1.
<Device> system-view
[Device] interface gigabitethernet 2/0/1
[Device-GigabitEthernet2/0/1] ipv6 verify source ip-address mac-address

On GigabitEthernet 2/0/1, configure a static IPv6SG binding for the host.
[Device-GigabitEthernet2/0/1] ipv6 source binding ip-address 2001::1 mac-address
0001-0202-0202
[Device-GigabitEthernet2/0/1] quit
```

## Verifying the configuration

# Verify that the static IPv6SG binding is configured successfully on the device.

```
[Device] display ipv6 source binding static
Total entries found: 1
IPv6 Address MAC Address Interface VLAN Type
2001::1 0001-0202-0202 GE2/0/1 N/A Static
```

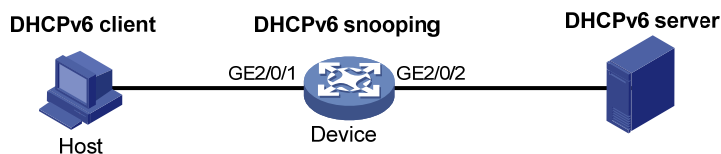
# Dynamic IPv6SG using DHCPv6 snooping configuration example

## Network requirements

As shown in [Figure 164](#):

- Enable DHCPv6 snooping on the device to record the IPv6 address and the MAC address of the host in a DHCPv6 snooping entry.
- Enable dynamic IPv6SG on GigabitEthernet 2/0/1 to filter received packets based on DHCPv6 snooping entries. Only packets from the client that obtains an IP address from the DHCPv6 server are allowed to pass.

**Figure 164 Network diagram**



## Configuration procedure

1. Configure DHCPv6 snooping:  
# Enable DHCPv6 snooping globally.  

```
<Device> system-view
[Device] ipv6 dhcp snooping enable
```

  
# Configure GigabitEthernet 2/0/2 as a trusted interface.  

```
[Device] interface gigabitethernet 2/0/2
[Device-GigabitEthernet2/0/2] ipv6 dhcp snooping trust
[Device-GigabitEthernet2/0/2] quit
```
2. Enable IPv6SG:  
# Enable IPv6SG on GigabitEthernet 2/0/1 and verify the source IP address and MAC address for dynamic IPv6SG.  

```
[Device] interface gigabitethernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] ipv6 verify source ip-address mac-address
Enable recording of client information in DHCPv6 snooping entries on GigabitEthernet 2/0/1.
[Device-GigabitEthernet2/0/1] ipv6 dhcp snooping binding record
[Device-GigabitEthernet2/0/1] quit
```

### Verifying the configuration

# Verify that a dynamic IPv6SG binding is generated based on a DHCPv6 snooping entry.

```
[Device] display ipv6 source binding dhcpv6-snooping
```

Total entries found: 1

| IPv6 Address | MAC Address    | Interface | VLAN | Type            |
|--------------|----------------|-----------|------|-----------------|
| 2001::1      | 040a-0000-0001 | GE2/0/1   | 1    | DHCPv6 snooping |



# Configuring ARP attack protection

ARP attacks and viruses are threatening LAN security. This chapter describes multiple features used to detect and prevent ARP attacks.

Although ARP is easy to implement, it provides no security mechanism and is vulnerable to network attacks. An attacker can exploit ARP vulnerabilities to attack network devices in the following ways:

- Acts as a trusted user or gateway to send ARP packets so the receiving devices obtain incorrect ARP entries.
- Sends a large number of unresolvable IP packets to have the receiving device busy with resolving IP addresses until its CPU is overloaded. Unresolvable IP packets refer to IP packets for which ARP cannot find corresponding MAC addresses.
- Sends a large number of ARP packets to overload the CPU of the receiving device.

For more information about ARP attack features and types, see *ARP Attack Protection Technology White Paper*.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## ARP attack protection configuration task list

| Tasks at a glance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Flood prevention:</p> <ul style="list-style-type: none"><li>• <a href="#">Configuring unresolvable IP attack protection</a> (configured on gateways)<ul style="list-style-type: none"><li>◦ <a href="#">Configuring ARP source suppression</a></li><li>◦ <a href="#">Enabling ARP blackhole routing</a></li></ul></li><li>• <a href="#">Configuring source MAC-based ARP attack detection</a> (configured on gateways)</li></ul>                                                                                                                                                                                                                                                                                             |
| <p>User and gateway spoofing prevention:</p> <ul style="list-style-type: none"><li>• <a href="#">Configuring ARP packet source MAC consistency check</a> (configured on gateways)</li><li>• <a href="#">Configuring ARP active acknowledgement</a> (configured on gateways)</li><li>• <a href="#">Configuring authorized ARP</a> (configured on gateways)</li><li>• <a href="#">Configuring ARP detection</a> (configured on access devices)</li><li>• <a href="#">Configuring ARP scanning and fixed ARP</a> (configured on gateways)</li><li>• <a href="#">Configuring ARP gateway protection</a> (configured on access devices)</li><li>• <a href="#">Configuring ARP filtering</a> (configured on access devices)</li></ul> |

# Configuring unresolvable IP attack protection

If a device receives a large number of unresolvable IP packets from a host, the following situations can occur:

- The device sends a large number of ARP requests, overloading the target subnets.
- The device keeps trying to resolve the destination IP addresses, overloading its CPU.

To protect the device from such IP attacks, you can configure the following features:

- **ARP source suppression**—Stops resolving packets from a host if the number of unresolvable IP packets from the host exceeds the upper limit within 5 seconds. The device continues ARP resolution when the interval elapses. This feature is applicable if the attack packets have the same source addresses.
- **ARP blackhole routing**—Creates a blackhole route destined for an unresolvable IP address. The device drops all matching packets until the blackhole route ages out. This feature is applicable regardless of whether the attack packets have the same source addresses.

## Configuring ARP source suppression

| Step                                                                                                        | Command                                                | Remarks                                         |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------|
| 1. Enter system view.                                                                                       | <b>system-view</b>                                     | N/A                                             |
| 2. Enable ARP source suppression.                                                                           | <b>arp source-suppression enable</b>                   | By default, ARP source suppression is disabled. |
| 3. Set the maximum number of unresolvable packets that the device can receive from a host within 5 seconds. | <b>arp source-suppression limit</b> <i>limit-value</i> | By default, the maximum number is 10.           |

## Enabling ARP blackhole routing

| Step                             | Command                           | Remarks                                       |
|----------------------------------|-----------------------------------|-----------------------------------------------|
| 1. Enter system view.            | <b>system-view</b>                | N/A                                           |
| 2. Enable ARP blackhole routing. | <b>arp resolving-route enable</b> | By default, ARP blackhole routing is enabled. |

## Displaying and maintaining unresolvable IP attack protection

Execute **display** commands in any view.

| Task                                                      | Command                               |
|-----------------------------------------------------------|---------------------------------------|
| Display ARP source suppression configuration information. | <b>display arp source-suppression</b> |

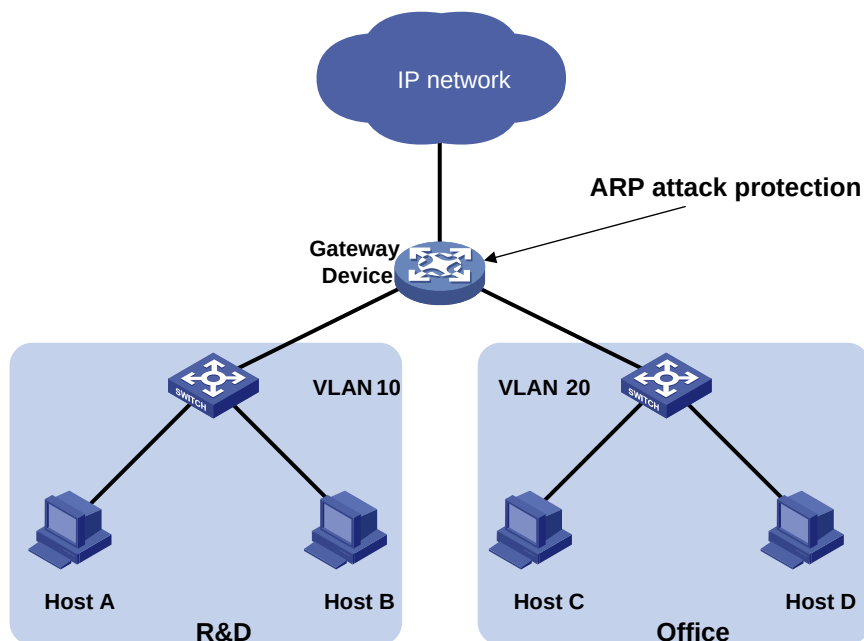
# Configuration example

## Network requirements

As shown in [Figure 165](#), a LAN contains two areas: an R&D area in VLAN 10 and an office area in VLAN 20. Each area connects to the gateway (Device) through an access switch.

A large number of ARP requests are detected in the office area and are considered an attack caused by unresolvable IP packets. To prevent the attack, configure ARP source suppression and ARP blackhole routing.

**Figure 165 Network diagram**



## Configuration considerations

If the attack packets have the same source address, configure the ARP source suppression feature as follows:

1. Enable ARP source suppression.
2. Set the threshold to 100. If the number of unresolvable IP packets received from a host within 5 seconds exceeds 100, the device stops resolving packets from the host until the 5 seconds elapse.

If the attack packets have different source addresses, enable the ARP blackhole routing feature on the gateway.

## Configuration procedure

# Enable ARP source suppression and set the threshold to 100.

```
<Device> system-view
```

```
[Device] arp source-suppression enable
```

```
[Device] arp source-suppression limit 100
```

# Enable ARP blackhole routing.

```
[Device] arp resolving-route enable
```

# Configuring source MAC-based ARP attack detection

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device adds the MAC address to an ARP attack entry. Before the entry is aged out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from that MAC address.

You can exclude the MAC addresses of some gateways and servers from this detection. This feature does not inspect ARP packets from those devices even if they are attackers.

## Configuration procedure

To configure source MAC-based ARP attack detection:

| Step                                                                             | Command                                                        | Remarks                                  |
|----------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------|
| 1. Enter system view.                                                            | <b>system-view</b>                                             | N/A                                      |
| 2. Enable source MAC-based ARP attack detection and specify the handling method. | <b>arp source-mac { filter   monitor }</b>                     | By default, this feature is disabled.    |
| 3. Set the threshold.                                                            | <b>arp source-mac threshold threshold-value</b>                | The default threshold is 30.             |
| 4. Set the aging timer for ARP attack entries.                                   | <b>arp source-mac aging-time time</b>                          | By default, the lifetime is 300 seconds. |
| 5. (Optional.) Exclude specific MAC addresses from this detection.               | <b>arp source-mac exclude-mac mac-address&amp;&lt;1-64&gt;</b> | By default, no MAC address is excluded.  |

### NOTE:

When an ARP attack entry is aged out, ARP packets sourced from the MAC address in the entry can be processed correctly.

## Displaying and maintaining source MAC-based ARP attack detection

Execute **display** commands in any view.

| Task                                                                                                                                                   | Command                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Display ARP attack entries detected by source MAC-based ARP attack detection (centralized devices in standalone mode).                                 | <b>display arp source-mac [ interface interface-type interface-number ]</b>                    |
| Display ARP attack entries detected by source MAC-based ARP attack detection (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display arp source-mac { slot slot-number   interface interface-type interface-number }</b> |

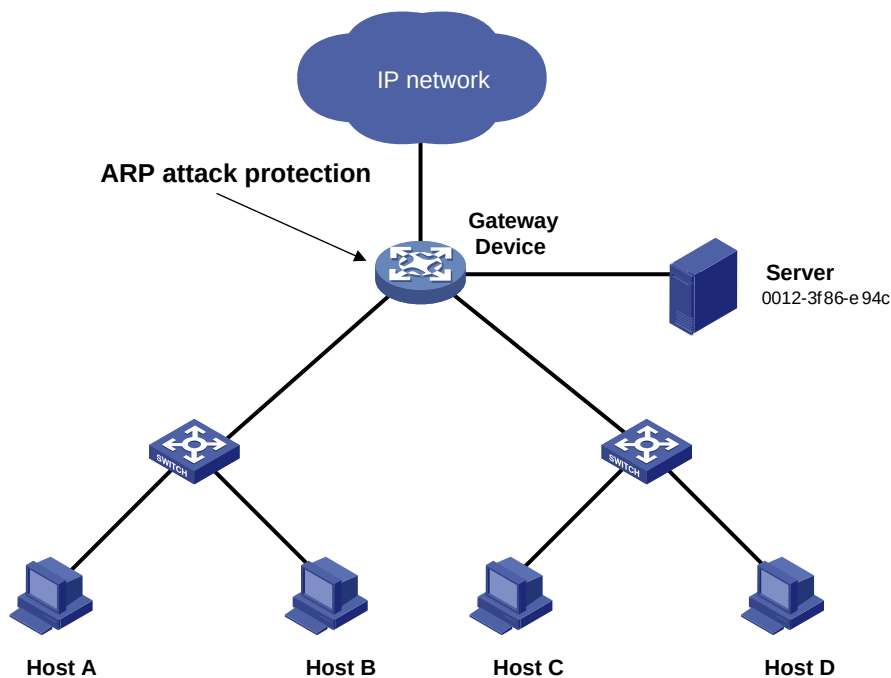
| Task                                                                                                            | Command                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display ARP attack entries detected by source MAC-based ARP attack detection (distributed devices in IRF mode). | <b>display arp source-mac</b> { <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i>   <b>interface</b> <i>interface-type</i> <i>interface-number</i> } |

## Configuration example

### Network requirements

As shown in Figure 166, the hosts access the Internet through a gateway (Device). If malicious users send a large number of ARP requests to the gateway, the gateway might crash and cannot process requests from the clients. To solve this problem, configure source MAC-based ARP attack detection on the gateway.

**Figure 166 Network diagram**



### Configuration considerations

An attacker might forge a large number of ARP packets by using the MAC address of a valid host as the source MAC address. To prevent such attacks, configure the gateway in the following steps:

1. Enable source MAC-based ARP attack detection and specify the handling method as filter.
2. Set the threshold.
3. Set the lifetime for ARP attack entries.
4. Exclude the MAC address of the server from this detection.

### Configuration procedure

# Enable source MAC-based ARP attack detection, and specify the handling method as filter.

```
<Device> system-view
```

```
[Device] arp source-mac filter
```

# Set the threshold to 30.

```
[Device] arp source-mac threshold 30
```

```
Set the lifetime for ARP attack entries to 60 seconds.
[Device] arp source-mac aging-time 60

Exclude MAC address 0012-3f86-e94c from this detection.
[Device] arp source-mac exclude-mac 0012-3f86-e94c
```

## Configuring ARP packet source MAC consistency check

This feature enables a gateway to filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body. This feature allows the gateway to learn correct ARP entries.

To enable ARP packet source MAC address consistency check:

| Step                                                       | Command                       | Remarks                                                                  |
|------------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------|
| 1. Enter system view.                                      | <b>system-view</b>            | N/A                                                                      |
| 2. Enable ARP packet source MAC address consistency check. | <b>arp valid-check enable</b> | By default, ARP packet source MAC address consistency check is disabled. |

## Configuring ARP active acknowledgement

Configure this feature on gateways to prevent user spoofing.

ARP active acknowledgement prevents a gateway from generating incorrect ARP entries.

In strict mode, a gateway performs more strict validity checks before creating an ARP entry:

- Upon receiving an ARP request destined for the gateway, the gateway sends an ARP reply but does not create an ARP entry.
- Upon receiving an ARP reply, the gateway determines whether it has resolved the sender IP address:
  - If yes, the gateway performs active acknowledgement. When the ARP reply is verified as valid, the gateway creates an ARP entry.
  - If no, the gateway discards the packet.

To configure ARP active acknowledgement:

| Step                                              | Command                                 | Remarks                               |
|---------------------------------------------------|-----------------------------------------|---------------------------------------|
| 1. Enter system view.                             | <b>system-view</b>                      | N/A                                   |
| 2. Enable the ARP active acknowledgement feature. | <b>arp active-ack [ strict ] enable</b> | By default, this feature is disabled. |

## Configuring authorized ARP

Authorized ARP entries are generated based on the DHCP clients' address leases on the DHCP server or dynamic client entries on the DHCP relay agent. For more information about DHCP server and DHCP relay agent, see *Layer 3—IP Services Configuration Guide*.

With authorized ARP enabled, an interface is disabled from learning dynamic ARP entries. This feature prevents user spoofing and allows only authorized clients to access network resources.

## Configuration procedure

To enable authorized ARP:

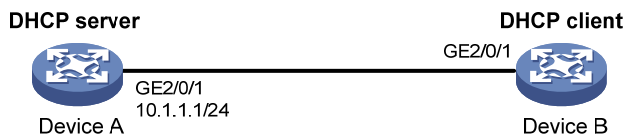
| Step                                       | Command                                                           | Remarks                                                                                                                                                                                                                                                                                   |
|--------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                      | <b>system-view</b>                                                | N/A                                                                                                                                                                                                                                                                                       |
| 2. Enter interface view.                   | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | The following interface types are supported: <ul style="list-style-type: none"> <li>• Layer 3 Ethernet interfaces.</li> <li>• Layer 3 Ethernet subinterfaces.</li> <li>• Layer 3 aggregate interfaces.</li> <li>• Layer 3 aggregate subinterfaces.</li> <li>• VLAN interfaces.</li> </ul> |
| 3. Enable authorized ARP on the interface. | <b>arp authorized enable</b>                                      | By default, authorized ARP is disabled.                                                                                                                                                                                                                                                   |

## Configuration example (on a DHCP server)

### Network requirements

As shown in [Figure 167](#), configure authorized ARP on GigabitEthernet 2/0/1 of Device A (a DHCP server) to ensure user validity.

**Figure 167 Network diagram**



### Configuration procedure

- Configure Device A:
  - # Specify the IP address for GigabitEthernet 2/0/1.
 

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet2/0/1] quit
```
  - # Configure DHCP.
 

```
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] quit
```
  - # Enter Layer 3 Ethernet interface view.
 

```
[DeviceA] interface gigabitethernet 2/0/1
```
  - # Enable authorized ARP.
 

```
[DeviceA-GigabitEthernet2/0/1] arp authorized enable
[DeviceA-GigabitEthernet2/0/1] quit
```

## 2. Configure Device B:

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address dhcp-alloc
[DeviceB-GigabitEthernet2/0/1] quit
```

### Verifying the configuration

# Display authorized ARP entry information on Device A.

```
[DeviceA] display arp all
```

| Type       | S-Static       | D-Dynamic | O-Openflow | R-Rule | M-Multiport | I-Invalid |
|------------|----------------|-----------|------------|--------|-------------|-----------|
| IP Address | MAC Address    | VLAN      | Interface  | Aging  | Type        |           |
| 10.1.1.2   | 0012-3f86-e94c | N/A       | GE2/0/1    | 20     | D           |           |

The output shows that IP address 10.1.1.2 has been assigned to Device B.

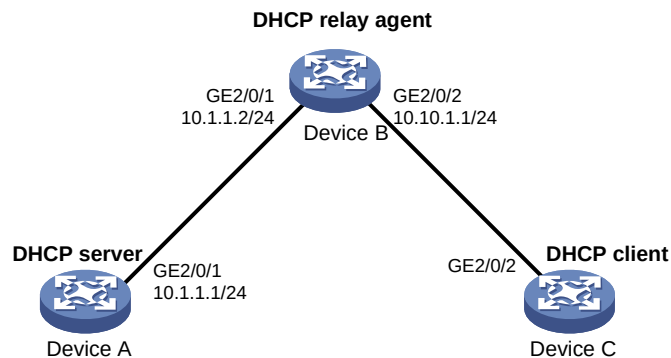
Device B must use the IP address and MAC address in the authorized ARP entry to communicate with Device A. Otherwise, the communication fails. Thus user validity is ensured.

## Configuration example (on a DHCP relay agent)

### Network requirements

As shown in [Figure 168](#), configure authorized ARP on GigabitEthernet 2/0/2 of Device B (a DHCP relay agent) to ensure user validity.

**Figure 168 Network diagram**



### Configuration procedure

#### 1. Configure Device A:

# Specify the IP address for GigabitEthernet 2/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet2/0/1] quit
```

# Configure DHCP.

```
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] gateway-list 10.10.1.1
[DeviceA-dhcp-pool-1] quit
[DeviceA] ip route-static 10.10.1.0 24 10.1.1.2
```



## 2. Configure Device B:

```
Enable DHCP.
<DeviceB> system-view
[DeviceB] dhcp enable

Specify the IP addresses of GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2.
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] ip address 10.1.1.2 24
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] ip address 10.10.1.1 24

Enable DHCP relay agent on GigabitEthernet 2/0/2.
[DeviceB-GigabitEthernet2/0/2] dhcp select relay

Add the DHCP server 10.1.1.1 to DHCP server group 1.
[DeviceB-GigabitEthernet2/0/2] dhcp relay server-address 10.1.1.1

Enable authorized ARP.
[DeviceB-GigabitEthernet2/0/2] arp authorized enable
[DeviceB-GigabitEthernet2/0/2] quit

Enable recording of relay entries on the relay agent.
[DeviceB] dhcp relay client-information record
```

## 3. Configure Device C:

```
<DeviceC> system-view
[DeviceC] ip route-static 10.1.1.0 24 10.10.1.1
[DeviceC] interface gigabitethernet 2/0/2
[DeviceC-GigabitEthernet2/0/2] ip address dhcp-alloc
[DeviceC-GigabitEthernet2/0/2] quit
```

### Verifying the configuration

# Display authorized ARP information on Device B.

```
[DeviceB] display arp all
```

| Type:      | S-Static       | D-Dynamic | O-Openflow | R-Rule | M-Multiport | I-Invalid |
|------------|----------------|-----------|------------|--------|-------------|-----------|
| IP Address | MAC Address    | VLAN      | Interface  | Aging  | Type        |           |
| 10.10.1.2  | 0012-3f86-e94c | N/A       | GE2/0/2    | 20     | D           |           |

The output shows that Device A assigned the IP address 10.10.1.2 to Device C.

Device C must use the IP address and MAC address in the authorized ARP entry to communicate with Device B. Otherwise, the communication fails. Thus the user validity is ensured.

## Configuring ARP detection

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
  - HMIM-8GSW.
  - HMIM-8GSWF.
  - HMIM-24GSW.
  - HMIM-24GSW-PoE.
  - SIC-4GSW.
  - SIC-4GSWP
- Fixed Layer 2 Ethernet ports on the following routers:

- MSR954(JH296A/JH297A/JH298A/JH299A).
- MSR1002-4/1003-8S.
- MSR2004-24/2004-48.

ARP detection enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks. ARP detection does not check ARP packets received from ARP trusted interfaces.

ARP detection provides the user validity check, ARP packet validity check, and ARP restricted forwarding features.

If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

## Configuring user validity check

Upon receiving an ARP packet from an ARP untrusted interface, the device matches the sender IP and MAC addresses with the following entries:

- Static IP source guard binding entries
- DHCP snooping entries

If a match is found, the ARP packet is considered valid and is forwarded. If no match is found, the ARP packet is considered invalid and is discarded.

Static IP source guard binding entries are created by using the **ip source binding** command. For more information, see "[Configuring IP source guard](#)."

DHCP snooping entries are automatically generated by DHCP snooping. For more information, see *Layer 3—IP Services Configuration Guide*.

### Configuration guidelines

When you configure user validity check, follow these guidelines:

- Make sure one or more of the following items is configured for user validity check:
  - Static IP source guard bindings.
  - DHCP snooping.

If none of the items is configured, all incoming ARP packets on ARP untrusted interfaces are discarded.

- You must specify a VLAN for an IP source guard binding entry. Otherwise, no ARP packets can match the IP source guard binding entry.

### Configuration procedure

To configure user validity check:

| Step                                                                          | Command                                                           | Remarks                                |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------|
| 1. Enter system view.                                                         | <b>system-view</b>                                                | N/A                                    |
| 2. Enter VLAN view.                                                           | <b>vlan</b> <i>vlan-id</i>                                        | N/A                                    |
| 3. Enable ARP detection.                                                      | <b>arp detection enable</b>                                       | By default, ARP detection is disabled. |
| 4. Return to system view.                                                     | <b>quit</b>                                                       | N/A                                    |
| 5. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view. | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                    |
| 6. (Optional.) Configure the interface as a trusted interface                 | <b>arp detection trust</b>                                        | By default, an interface is untrusted. |

| Step                         | Command | Remarks |
|------------------------------|---------|---------|
| excluded from ARP detection. |         |         |

## Configuring ARP packet validity check

Enable validity check for ARP packets received on untrusted interfaces and specify the following objects to be checked:

- **src-mac**—Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.
- **dst-mac**—Checks the target MAC address of ARP replies. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.
- **ip**—Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

To configure ARP packet validity check:

| Step                                                                                       | Command                                                                               | Remarks                                            |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------|
| 1. Enter system view.                                                                      | <b>system-view</b>                                                                    | N/A                                                |
| 2. Enter VLAN view.                                                                        | <b>vlan</b> <i>vlan-id</i>                                                            | N/A                                                |
| 3. Enable ARP detection.                                                                   | <b>arp detection enable</b>                                                           | By default, ARP detection is disabled.             |
| 4. Return to system view.                                                                  | <b>quit</b>                                                                           | N/A                                                |
| 5. Enable ARP packet validity check and specify the objects to be checked.                 | <b>arp detection validate</b><br>{ <b>dst-mac</b>   <b>ip</b>   <b>src-mac</b> }<br>* | By default, ARP packet validity check is disabled. |
| 6. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.              | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                     | N/A                                                |
| 7. (Optional.) Configure the interface as a trusted interface excluded from ARP detection. | <b>arp detection trust</b>                                                            | By default, an interface is untrusted.             |

## Configuring ARP restricted forwarding

### NOTE:

ARP restricted forwarding does not apply to ARP packets with multiport MAC as their destination MAC addresses.

ARP restricted forwarding controls the forwarding of ARP packets that are received on untrusted interfaces and have passed user validity check as follows:

- If the packets are ARP requests, they are forwarded through the trusted interface.
- If the packets are ARP replies, they are forwarded according to their destination MAC address. If no match is found in the MAC address table, they are forwarded through the trusted interface.

Configure user validity check before you configure ARP restricted forwarding.

To enable ARP restricted forwarding:

| Step                                 | Command                                 | Remarks                                            |
|--------------------------------------|-----------------------------------------|----------------------------------------------------|
| 1. Enter system view.                | <b>system-view</b>                      | N/A                                                |
| 2. Enter VLAN view.                  | <b>vlan <i>vlan-id</i></b>              | N/A                                                |
| 3. Enable ARP restricted forwarding. | <b>arp restricted-forwarding enable</b> | By default, ARP restricted forwarding is disabled. |

## Displaying and maintaining ARP detection

Execute **display** commands in any view and **reset** commands in user view.

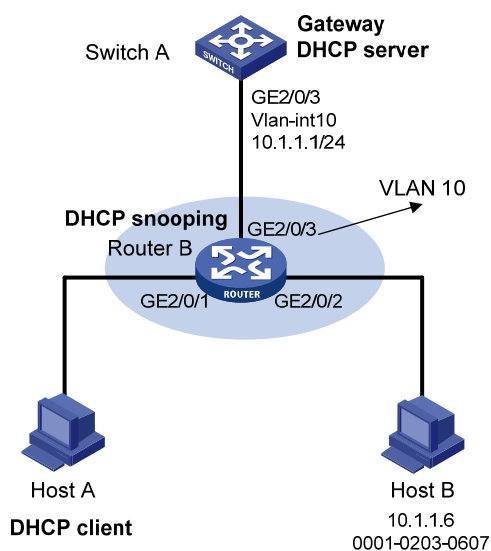
| Task                                          | Command                                                                                             |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Display the VLANs enabled with ARP detection. | <b>display arp detection</b>                                                                        |
| Display the ARP detection statistics.         | <b>display arp detection statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ] |
| Clear the ARP detection statistics.           | <b>reset arp detection statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]   |

## User validity check and ARP packet validity check configuration example

### Network requirements

As shown in Figure 169, configure Router B to perform ARP packet validity check and user validity check based on static IP source guard binding entries and DHCP snooping entries for connected hosts.

Figure 169 Network diagram



### Configuration procedure

1. Add all interfaces on Router B to VLAN 10, and specify the IP address of VLAN-interface 10 on Switch A. (Details not shown.)
2. Configure the DHCP server on Switch A, and configure DHCP address pool 0.

```

<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0

```

3. Configure Host A (DHCP client) and Host B. (Details not shown.)

4. Configure Router B:

```

Enable DHCP snooping.
<RouterB> system-view
[RouterB] dhcp snooping enable
[RouterB] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] dhcp snooping trust
[RouterB-GigabitEthernet2/0/3] quit
Enable recording of client information in DHCP snooping entries on GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] dhcp snooping binding record
[RouterB-GigabitEthernet2/0/1] quit
Enable ARP detection for VLAN 10.
[RouterB] vlan 10
[RouterB-vlan10] arp detection enable
Configure the upstream interface as a trusted interface. By default, an interface is an
untrusted interface.
[RouterB-vlan10] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] arp detection trust
[RouterB-GigabitEthernet2/0/3] quit
Configure a static IP source guard binding entry on interface GigabitEthernet 2/0/2 for user
validity check.
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[RouterB-GigabitEthernet2/0/2] quit
Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP
packets.
[RouterB] arp detection validate dst-mac ip src-mac

```

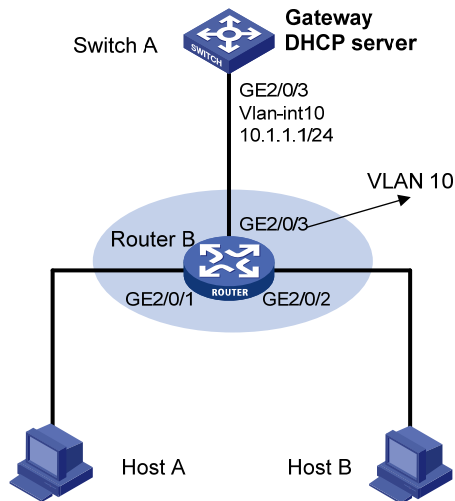
After the configurations are completed, Router B first checks the validity of ARP packets received on GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2. If the ARP packets are confirmed valid, the router performs user validity check by using the static IP source guard binding entries and finally DHCP snooping entries.

## ARP restricted forwarding configuration example

### Network requirements

As shown in [Figure 170](#), configure ARP restricted forwarding on Router B where ARP detection is configured. Port isolation configured on Router B can take effect for broadcast ARP requests.

**Figure 170 Network diagram**



### Configuration procedure

1. Configure VLAN 10, add interfaces to VLAN 10, and specify the IP address of the VLAN interface. (Details not shown.)
2. Configure the DHCP server on Switch A, and configure DHCP address pool 0.
 

```
<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```
3. Configure Host A (DHCP client) and Host B. (Details not shown.)
4. Configure Router B:
 

```
Enable DHCP snooping, and configure GigabitEthernet 2/0/3 as a DHCP trusted interface.
<RouterB> system-view
[RouterB] dhcp snooping enable
[RouterB] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] dhcp snooping trust
[RouterB-GigabitEthernet2/0/3] quit

Enable ARP detection for user validity check.
[RouterB] vlan 10
[RouterB-vlan10] arp detection enable

Configure GigabitEthernet 2/0/3 as an ARP trusted interface.
[RouterB-vlan10] interface gigabitethernet 2/0/3
[RouterB-GigabitEthernet2/0/3] arp detection trust
[RouterB-GigabitEthernet2/0/3] quit

Configure a static IP source guard entry on interface GigabitEthernet 2/0/2.
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[RouterB-GigabitEthernet2/0/2] quit

Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.
[RouterB] arp detection validate dst-mac ip src-mac

Configure port isolation.
```

```
[RouterB] port-isolate group 1
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] port-isolate enable group 1
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] port-isolate enable group 1
[RouterB-GigabitEthernet2/0/2] quit
```

After the configurations are completed, Router B first checks the validity of ARP packets received on GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2. If the ARP packets are confirmed valid, the router performs user validity check by using the static IP source guard binding entries and finally DHCP snooping entries. However, ARP broadcast requests sent from Host A can pass the check on Router B and reach Host B. Port isolation fails.

# Enable ARP restricted forwarding.

```
[RouterB] vlan 10
[RouterB-vlan10] arp restricted-forwarding enable
[RouterB-vlan10] quit
```

After the configuration is completed, Router B forwards ARP broadcast requests from Host A to Switch A through the trusted interface GigabitEthernet 2/0/3. Host B cannot receive such packets. Port isolation operates correctly.

## Configuring ARP scanning and fixed ARP

ARP scanning is typically used together with the fixed ARP feature in small-scale networks.

ARP scanning automatically creates ARP entries for devices in an address range. The device performs ARP scanning in the following steps:

1. Sends ARP requests for each IP address in the address range.
2. Obtains their MAC addresses through received ARP replies.
3. Creates dynamic ARP entries.

Fixed ARP converts existing dynamic ARP entries (including those generated through ARP scanning) to static ARP entries. This feature prevents ARP entries from being modified by attackers. Static ARP entries can also be manually configured by the **arp static** command.

## Configuration restrictions and guidelines

Follow these restrictions and guidelines when you configure ARP scanning and fixed ARP:

- IP addresses in existing ARP entries are not scanned.
- ARP scanning will take some time. To stop an ongoing scan, press **Ctrl + C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.
- The **arp fixup** command is a one-time operation. You can use this command again to convert the dynamic ARP entries learned later to static.
- Due to the limit on the total number of static ARP entries, some dynamic ARP entries might fail the conversion.
- To delete a static ARP entry converted from a dynamic one, use the **undo arp ip-address [ vpn-instance-name ]** command. Use the **reset arp all** command to delete all ARP entries or the **reset arp static** command to delete all static ARP entries.

## Configuration procedure

To configure ARP scanning and fixed ARP:

| Step                      | Command                                                       |
|---------------------------|---------------------------------------------------------------|
| 1. Enter system view.     | <b>system-view</b>                                            |
| 2. Enter interface view.  | <b>interface</b> <i>interface-type interface-number</i>       |
| 3. Enable ARP scanning.   | <b>arp scan</b> [ <i>start-ip-address to end-ip-address</i> ] |
| 4. Return to system view. | <b>quit</b>                                                   |
| 5. Enable fixed ARP.      | <b>arp fixup</b>                                              |

## Configuring ARP gateway protection

Configure this feature on interfaces not connected with a gateway to prevent gateway spoofing attacks.

When such an interface receives an ARP packet, it checks whether the sender IP address in the packet is consistent with that of any protected gateway. If yes, it discards the packet. If not, it handles the packet correctly.

## Configuration guidelines

Follow these guidelines when you configure ARP gateway protection:

- You can enable ARP gateway protection for a maximum of eight gateways on an interface.
- Do not configure both the **arp filter source** and **arp filter binding** commands on an interface.
- If ARP gateway protection operates with ARP detection and ARP fast-reply, ARP gateway protection applies first.

## Configuration procedure

To configure ARP gateway protection:

| Step                                                                      | Command                                                 | Remarks                                         |
|---------------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------|
| 1. Enter system view.                                                     | <b>system-view</b>                                      | N/A                                             |
| 2. Enter Layer 2 Ethernet interface and Layer 2 aggregate interface view. | <b>interface</b> <i>interface-type interface-number</i> | N/A                                             |
| 3. Enable ARP gateway protection for the specified gateway.               | <b>arp filter source</b> <i>ip-address</i>              | By default, ARP gateway protection is disabled. |

## Configuration example

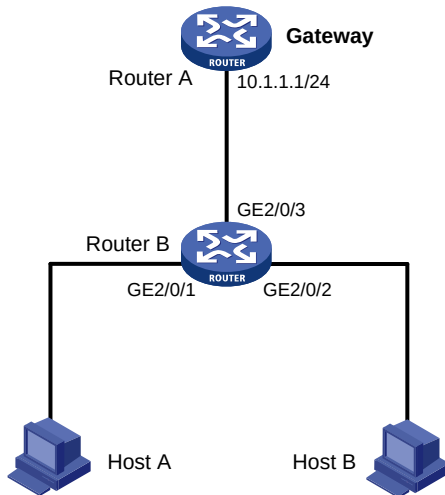
### Network requirements

As shown in [Figure 171](#), Host B launches gateway spoofing attacks to Router B. As a result, traffic that Router B intends to send to Router A is sent to Host B.

Configure Router B to block such attacks.



**Figure 171 Network diagram**



### Configuration procedure

# Configure ARP gateway protection on Router B.

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] arp filter source 10.1.1.1
[RouterB-GigabitEthernet2/0/1] quit
[RouterB] interface gigabitethernet 2/0/2
[RouterB-GigabitEthernet2/0/2] arp filter source 10.1.1.1
```

### Verifying the configuration

# Verify that GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2 discard the incoming ARP packets whose sender IP address is the IP address of the gateway.

## Configuring ARP filtering

The ARP filtering feature can prevent gateway spoofing and user spoofing attacks.

An interface enabled with this feature checks the sender IP and MAC addresses in a received ARP packet against permitted entries. If a match is found, the packet is handled correctly. If not, the packet is discarded.

## Configuration guidelines

Follow these guidelines when you configure ARP filtering:

- You can configure a maximum of eight permitted entries on an interface.
- Do not configure both the **arp filter source** and **arp filter binding** commands on an interface.
- If ARP filtering operates with ARP detection and ARP fast-reply, ARP filtering applies first.

## Configuration procedure

To configure ARP filtering:

| Step                                                                     | Command                                                           | Remarks                                |
|--------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------|
| 1. Enter system view.                                                    | <b>system-view</b>                                                | N/A                                    |
| 2. Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view. | <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | N/A                                    |
| 3. Enable ARP filtering and configure a permitted entry.                 | <b>arp filter binding</b> <i>ip-address</i><br><i>mac-address</i> | By default, ARP filtering is disabled. |

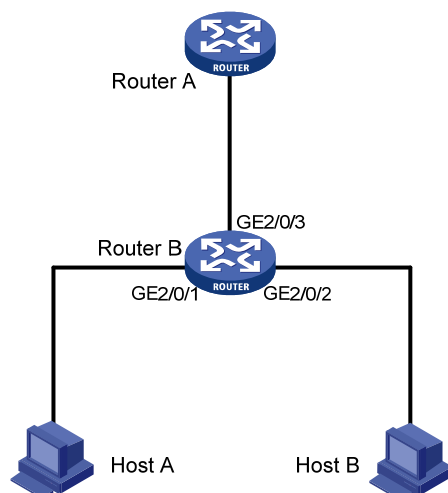
## Configuration example

### Network requirements

As shown in Figure 172, the IP and MAC addresses of Host A are 10.1.1.2 and 000f-e349-1233, respectively. The IP and MAC addresses of Host B are 10.1.1.3 and 000f-e349-1234, respectively.

Configure ARP filtering on GigabitEthernet 2/0/1 and GigabitEthernet 2/0/2 of Router B to permit ARP packets from only Host A and Host B.

**Figure 172 Network diagram**



### Configuration procedure

# Configure ARP filtering on Router B.

```
<RouterB> system-view
```

```
[RouterB] interface gigabitethernet 2/0/1
```

```
[RouterB-GigabitEthernet2/0/1] arp filter binding 10.1.1.2 000f-e349-1233
```

```
[RouterB-GigabitEthernet2/0/1] quit
```

```
[RouterB] interface gigabitethernet 2/0/2
```

```
[RouterB-GigabitEthernet2/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

### Verifying the configuration

# Verify that GigabitEthernet 2/0/1 permits ARP packets from Host A and discards other ARP packets.

# Verify that GigabitEthernet 2/0/2 permits ARP packets from Host B and discards other ARP packets.

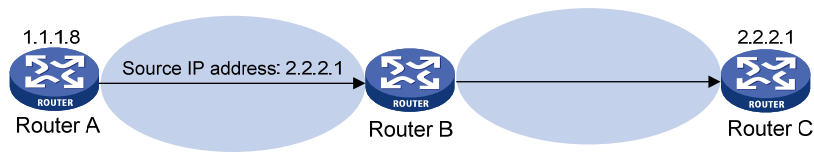
# Configuring uRPF

## Overview

Unicast Reverse Path Forwarding (uRPF) protects a network against source address spoofing attacks, such as DoS and DDoS attacks.

Attackers send packets with a forged source address to access a system that uses IP-based authentication, in the name of authorized users or even the administrator. Even if the attackers or other hosts cannot receive any response packets, the attacks are still disruptive to the attacked target.

**Figure 173 Source address spoofing attack**



As shown in [Figure 173](#), an attacker on Router A sends the server (Router B) requests with a forged source IP address 2.2.2.1 at a high rate. Router B sends response packets to IP address 2.2.2.1 (Router C). Consequently, both Router B and Router C are attacked. If the administrator disconnects Router C by mistake, the network service is interrupted.

Attackers can also send packets with different forged source addresses or attack multiple servers simultaneously to block connections or even break down the network.

uRPF can prevent these source address spoofing attacks. It checks whether an interface that receives a packet is the output interface of the FIB entry that matches the source address of the packet. If not, uRPF considers it a spoofing attack and discards the packet.

## uRPF check modes

uRPF supports strict and loose modes.

- **Strict uRPF check**—To pass strict uRPF check, the source address of a packet and the receiving interface must match the destination address and output interface of a FIB entry. In some scenarios (for example, asymmetrical routing), strict uRPF might discard valid packets. Strict uRPF is often deployed between a PE and a CE.
- **Loose uRPF check**—To pass loose uRPF check, the source address of a packet must match the destination address of a FIB entry. Loose uRPF can avoid discarding valid packets, but might let go attack packets. Loose uRPF is often deployed between ISPs, especially in asymmetrical routing.

## Features

**Default route**—When a default route exists, all packets that fail to match a specific FIB entry match the default route during uRPF check and thus are permitted to pass. To avoid this situation, you can disable uRPF from using any default route to discard such packets. If you allow using the default route (set by using **allow-default-route**), uRPF permits packets that only match the default route. By default, uRPF discards packets that can only match a default route. Typically, you do not need to configure the **allow-default-route** keyword on a PE device because it has no default route pointing to the CE. If you enable uRPF on a CE that has a default route pointing to the PE, select the **allow-default-route** keyword.

**Link layer check**—Strict uRPF check can further perform link layer check on a packet. It uses the next hop address in the matching FIB entry to look up the ARP table for a matching entry. If the source MAC address of the packet matches the MAC address in the matching ARP entry, the packet passes strict uRPF check. Link layer check is applicable to ISP devices where a Layer 3 Ethernet interface connects a large number of PCs. Loose uRPF does not support link layer check.

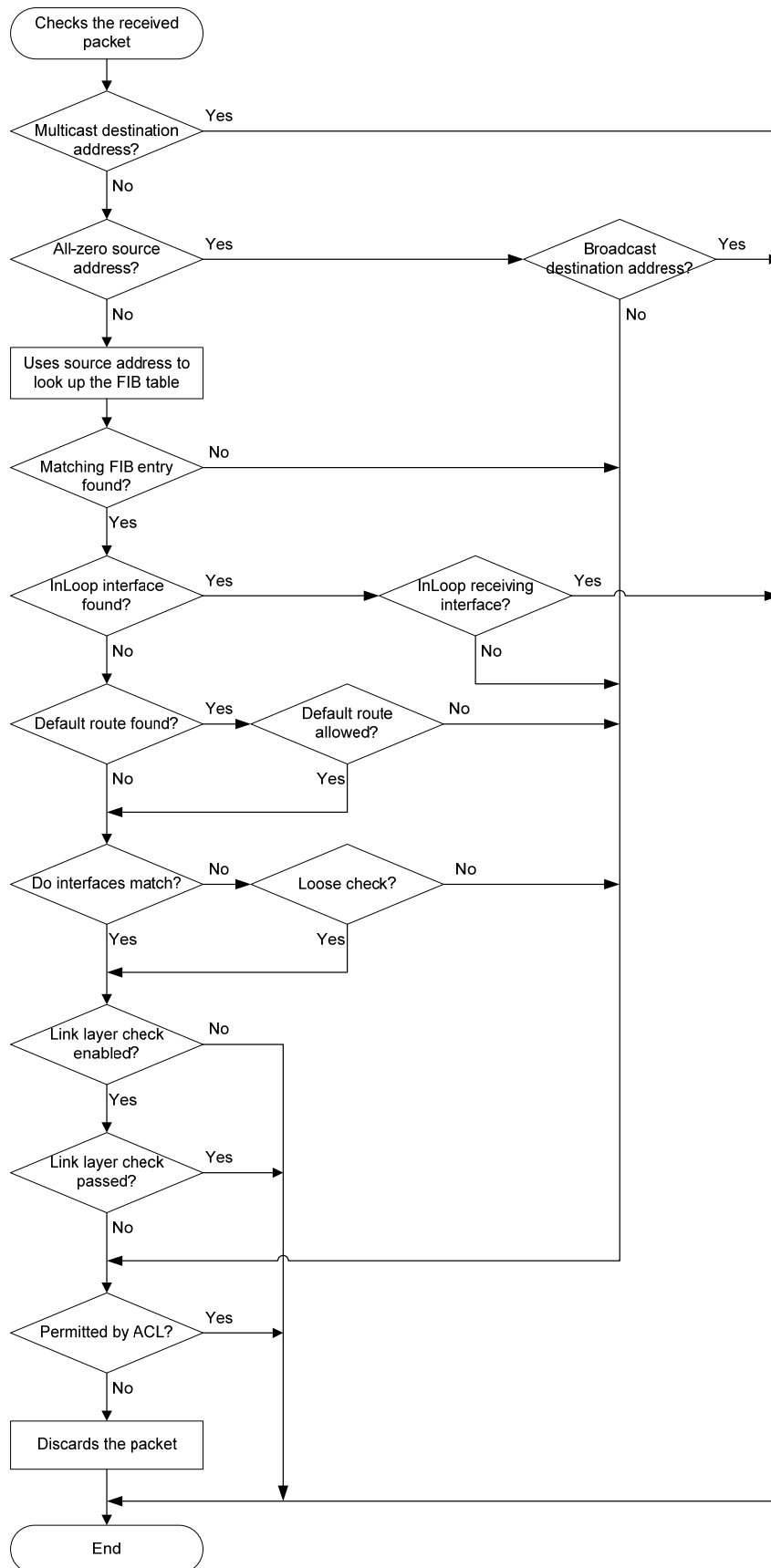
**ACL**—To identify specific packets as valid packets, you can use an ACL to match these packets. Even if the packets do not pass uRPF check, they are still forwarded.

## uRPF operation

uRPF does not check multicast packets.

Figure 174 shows how uRPF works.

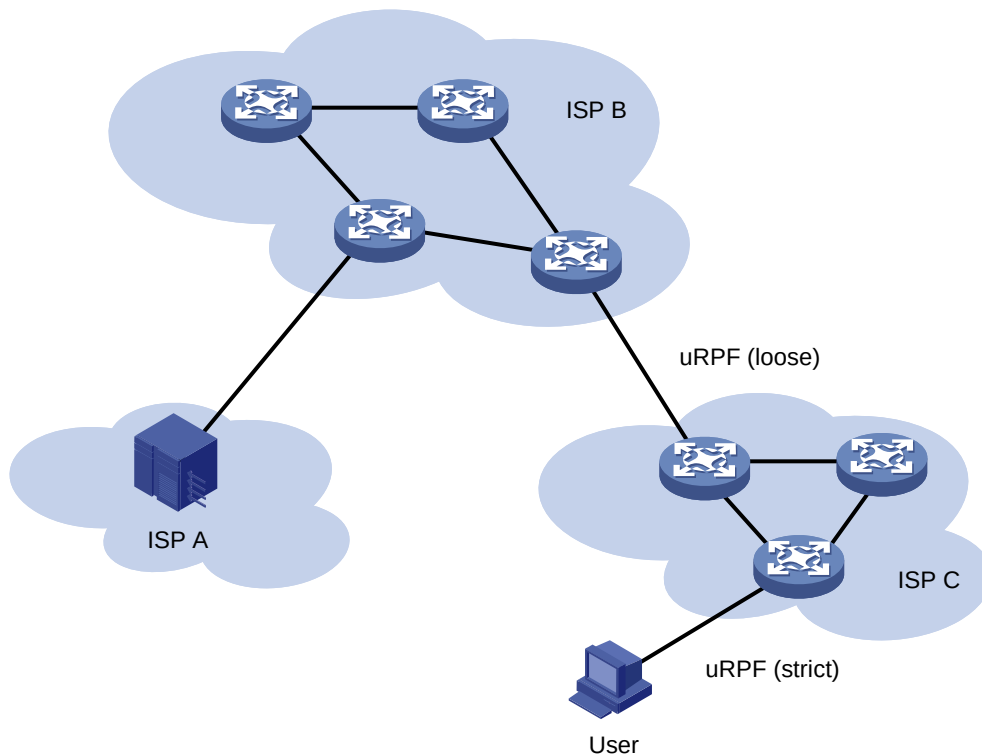
**Figure 174 uRPF work flow**



1. uRPF checks address validity:
  - uRPF permits a packet with a multicast destination address.
  - For a packet with an all-zero source address, uRPF permits the packet if it has a broadcast destination address. (A packet with source address 0.0.0.0 and destination address 255.255.255.255 might be a DHCP or BOOTP packet and cannot be discarded.) uRPF proceeds to step 7 if the packet has a non-broadcast destination address.
  - uRPF proceeds to step 2 for other packets.
2. uRPF checks whether the source address matches a unicast route:
  - If yes, uRPF proceeds to step 3.
  - If no, uRPF proceeds to step 7. A non-unicast source address matches a non-unicast route.
3. uRPF checks whether the matching route is to the host itself:
  - If yes, the output interface of the matching route is an InLoop interface. uRPF checks whether the receiving interface of the packet is an InLoop interface. If yes, it does not check the packet. If no, it proceeds to step 7.
  - If no, uRPF proceeds to step 4.
4. uRPF checks whether the matching route is a default route:
  - If yes, uRPF checks whether the **allow-default-route** keyword is configured to allow using the default route. If yes, it proceeds to step 5. If no, it proceeds to step 7.
  - If no, uRPF proceeds to step 5.
5. uRPF checks whether the receiving interface matches the output interface of the matching FIB entry:
  - If yes, uRPF proceeds to step 6.
  - If no, uRPF checks whether the check mode is loose. If yes, it proceeds to step 6. If no, it proceeds to step 7.
6. uRPF checks whether the **link-check** keyword is configured for link layer check:
  - If no, the packet passes the check.
  - If yes, uRPF uses the next-hop address of the FIB entry to look up the ARP table for a matching entry. Then it checks whether the MAC address of the matching ARP entry is identical with the source MAC address of the packet. If yes, the packet passes the check. If no, uRPF proceeds to step 7.
7. uRPF checks whether the packet is permitted by the ACL:
  - If yes, the packet is forwarded (such a packet is displayed in the uRPF information as a "suppressed drop").
  - If no, the packet is discarded.

# Network application

Figure 175 Network diagram



As shown in [Figure 175](#), strict uRPF check is configured between an ISP network and a customer network. Loose uRPF check is configured between ISPs.

For special packets or users, you can configure ACLs.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Configuring uRPF

A device supports uRPF configuration only on interfaces.

Follow these guidelines when you configure uRPF:

- uRPF checks only incoming packets on interfaces.
- You can use the **display ip interface** command to display statistics about packets discarded by uRPF (displayed as "Drops" and "Suppressed drops").

- Do not configure the **allow-default-route** keyword for loose uRPF check. Otherwise, uRPF might fail to work.

To enable uRPF on an interface:

| Step                             | Command                                                                                                                                                                                                    | Remarks                       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 1. Enter system view.            | <b>system-view</b>                                                                                                                                                                                         | N/A                           |
| 2. Enter interface view.         | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                                                                                                          | N/A                           |
| 3. Enable uRPF on the interface. | <b>ip urpf { loose</b><br>[ <b>allow-default-route</b> ] [ <b>acl</b><br><i>acl-number</i> ]   <b>strict</b><br>[ <b>allow-default-route</b> ] [ <b>acl</b><br><i>acl-number</i> ] [ <b>link-check</b> ] } | By default, uRPF is disabled. |

## Displaying and maintaining uRPF

Execute **display** commands in any view.

| Task                                                                                                 | Command                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display uRPF configuration (centralized devices in standalone mode).                                 | <b>display ip urpf</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]                                                                            |
| Display uRPF configuration (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display ip urpf</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]<br>[ <b>slot</b> <i>slot-number</i> ]                                      |
| Display uRPF configuration (distributed devices in IRF mode).                                        | <b>display ip urpf</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]<br>[ <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] |

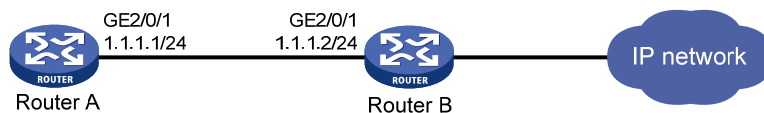
## uRPF configuration example

### Network requirements

As shown in Figure 176, configure strict uRPF check on GigabitEthernet 2/0/1 of Router B and permit packets from network 10.1.1.0/24.

Configure strict uRPF check on GigabitEthernet 2/0/1 of Router A and allow using the default route for uRPF check.

**Figure 176 Network diagram**



### Configuration procedure

- Configure Router B:
  - # Define ACL 2010 to permit traffic from network 10.1.1.0/24.
  - <RouterB> system-view
  - [RouterB] acl basic 2010
  - [RouterB-acl-ipv4-basic-2010] rule permit source 10.1.1.0 0.0.0.255
  - [RouterB-acl-ipv4-basic-2010] quit



```
Specify the IP address of GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ip address 1.1.1.2 255.255.255.0
Configure strict uRPF check on GigabitEthernet 2/0/1.
[RouterB-GigabitEthernet2/0/1] ip urpf strict acl 2010
```

**2. Configure Router A:**

```
Specify the IP address of GigabitEthernet 2/0/1.
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ip address 1.1.1.1 255.255.255.0
Configure strict uRPF check on GigabitEthernet 2/0/1 and allow use of the default route for
uRPF check.
[RouterA-GigabitEthernet2/0/1] ip urpf strict allow-default-route
```

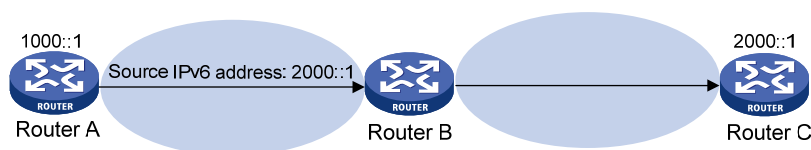
# Configuring IPv6 uRPF

## Overview

Unicast Reverse Path Forwarding (uRPF) protects a network against source address spoofing attacks, such as DoS and DDoS attacks.

Attackers send packets with a forged source address to access a system that uses IP-based authentication, in the name of authorized users or even the administrator. Even if the attackers or other hosts cannot receive any response packets, the attacks are still disruptive to the attacked target.

**Figure 177 Source address spoofing attack**



As shown in [Figure 177](#), an attacker on Router A sends the server (Router B) requests with a forged source IPv6 address 2000::1 at a high rate. Router B sends response packets to IPv6 address 2000::1 (Router C). Consequently, both Router B and Router C are attacked. If the administrator disconnects Router C by mistake, the network service is interrupted.

Attackers can also send packets with different forged source addresses or attack multiple servers simultaneously to block connections or even break down the network.

IPv6 uRPF can prevent these source address spoofing attacks. It checks whether an interface that receives a packet is the output interface of the FIB entry that matches the source address of the packet. If not, uRPF considers it a spoofing attack and discards the packet.

## IPv6 uRPF check modes

IPv6 uRPF supports strict and loose check modes.

- **Strict IPv6 uRPF check**—To pass strict IPv6 uRPF check, the source address of a packet and the receiving interface must match the destination address and output interface of an IPv6 FIB entry. In some scenarios (for example, asymmetrical routing), strict IPv6 uRPF might discard valid packets. Strict IPv6 uRPF is often deployed between a PE and a CE.
- **Loose IPv6 uRPF check**—To pass loose IPv6 uRPF check, the source address of a packet must match the destination address of an IPv6 FIB entry. Loose IPv6 uRPF can avoid discarding valid packets, but might let go attack packets. Loose IPv6 uRPF is often deployed between ISPs, especially in asymmetrical routing.

## Features

**Default route**—When a default route exists, all packets that fail to match a specific IPv6 FIB entry match the default route during IPv6 uRPF check and thus are permitted to pass. If you allow using the default route (by using **allow-default-route**), IPv6 uRPF permits packets that only match the default route. By default, IPv6 uRPF discards packets that can only match a default route. Typically, you do not need to configure the **allow-default-route** keyword on a PE device because it has no default route pointing to the CE device. If you enable IPv6 uRPF on a CE that has a default route pointing to the PE, select the **allow-default-route** keyword.

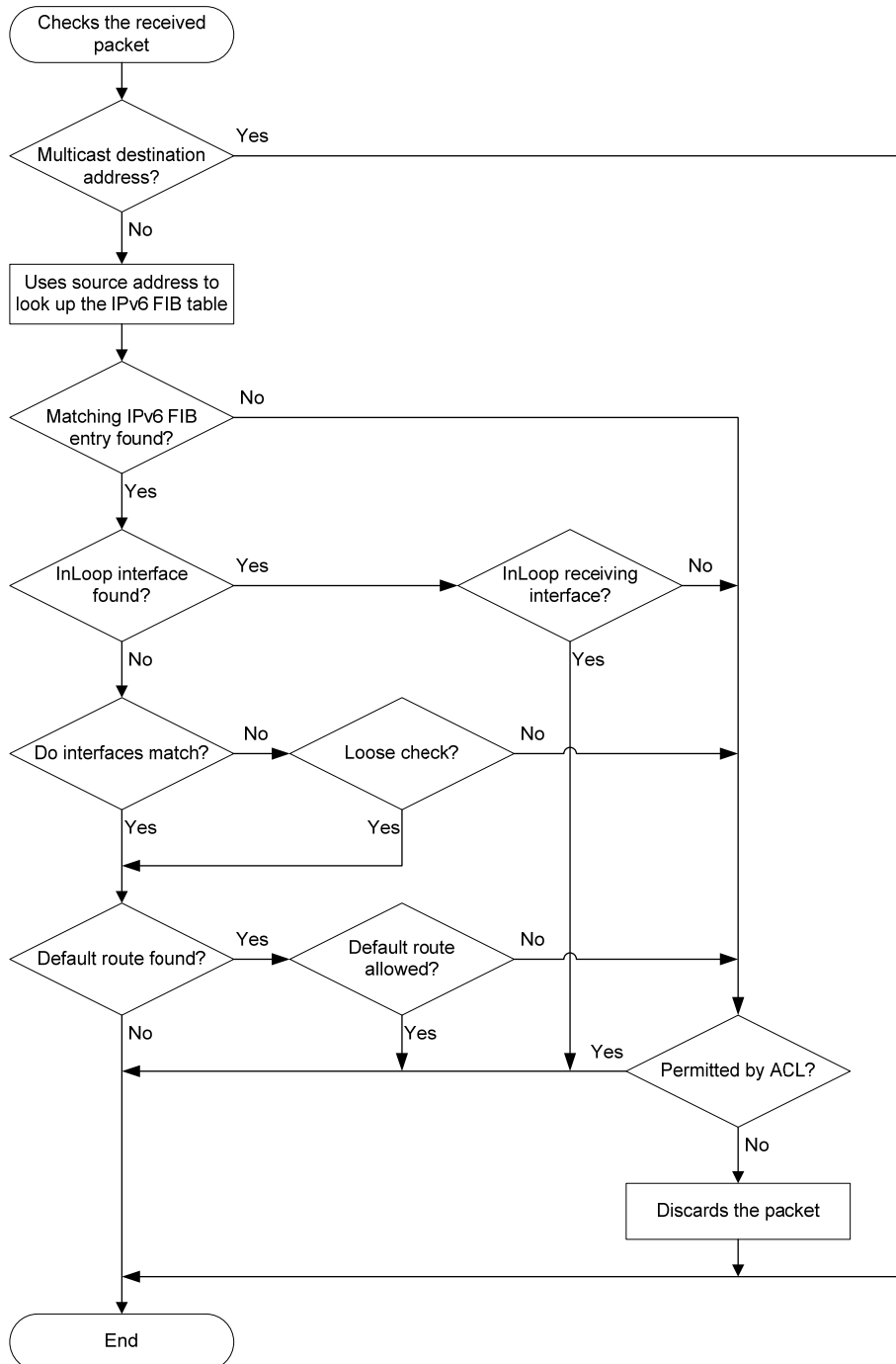
**IPv6 ACLs**—To identify specific packets as valid packets, you can use an IPv6 ACL to match these packets. Even if the packets do not pass IPv6 uRPF check, they are still forwarded.

## IPv6 uRPF operation

IPv6 uRPF does not check multicast packets.

Figure 178 shows how IPv6 uRPF works.

### Figure 178 IPv6 uRPF work flow

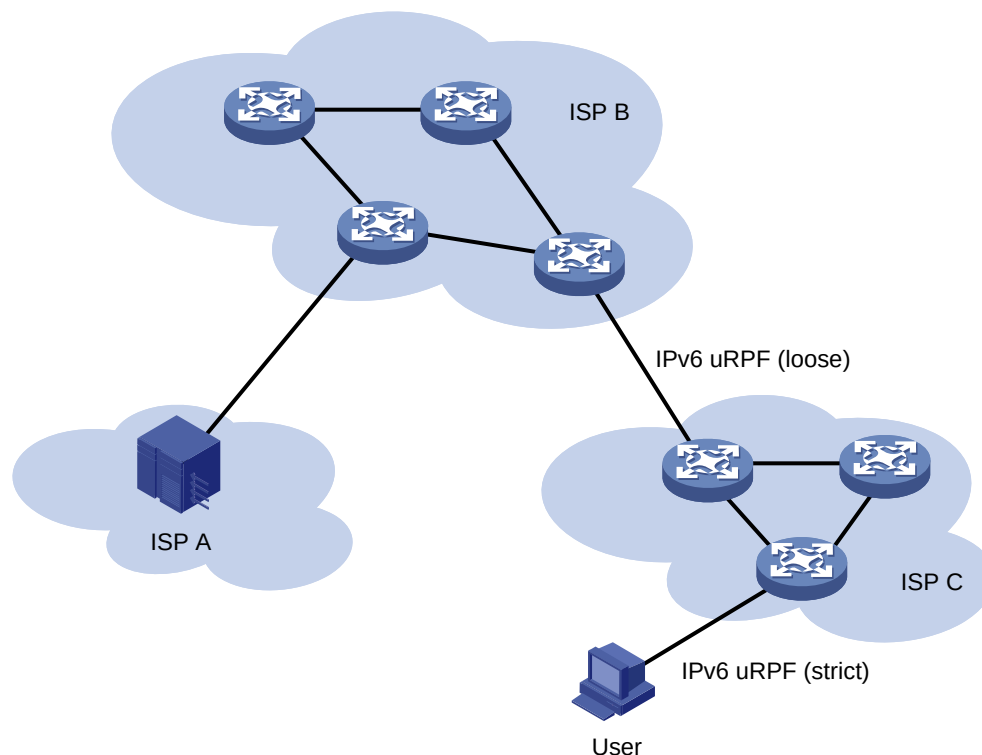


1. IPv6 uRPF checks whether the received packet carries a multicast destination address:
  - o If yes, IPv6 uRPF permits the packet.

- If no, IPv6 uRPF proceeds to step 2.
- 2. IPv6 uRPF checks whether the source address matches a unicast route:
  - If yes, IPv6 uRPF proceeds to step 3.
  - If no, IPv6 uRPF proceeds to step 6. A non-unicast source address matches a non-unicast route.
- 3. IPv6 uRPF checks whether the matching route is to the host itself:
  - If yes, the output interface of the matching route is an InLoop interface. IPv6 uRPF checks whether the receiving interface of the packet is an InLoop interface. If yes, IPv6 uRPF permits the packet. If no, IPv6 uRPF proceeds to step 6. If the source address is a link-local address and is the receiving interface address, also proceeds to step 6.
  - If no, IPv6 uRPF proceeds to step 4.
- 4. IPv6 uRPF checks whether the receiving interface matches the output interface of the matching FIB entry:
  - If yes, IPv6 uRPF proceeds to step 5.
  - If no, IPv6 uRPF checks whether the check mode is loose. If yes, it proceeds to step 5. If no, it proceeds to step 6.
- 5. IPv6 uRPF checks whether the matching route is a default route:
  - If yes, IPv6 uRPF checks whether the **allow-default-route** keyword is configured to allow using the default route. If yes, the packet is forwarded. If no, IPv6 uRPF proceeds to step 6.
  - If no, the packet is forwarded.
- 6. IPv6 uRPF checks whether the packet is permitted by the IPv6 ACL:
  - If yes, the packet is forwarded (such a packet is displayed in the uRPF information as a "suppressed drop").
  - If no, the packet is discarded.

# Network application

Figure 179 Network diagram



As shown in [Figure 179](#), strict IPv6 uRPF check is configured between an ISP network and a customer network. Loose IPv6 uRPF check is configured between ISPs.

For special packets or users, you can configure IPv6 ACLs.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Configuring IPv6 uRPF

A device supports IPv6 uRPF configuration only on interfaces.

Follow these guidelines when you configure IPv6 uRPF:

- IPv6 uRPF checks only incoming packets on interfaces.
- You can use the **display ipv6 interface** command to display statistics about packets discarded by IPv6 uRPF (displayed as "Drops" and "Suppressed drops").

- Do not configure the **allow-default-route** keyword for loose IPv6 uRPF check. Otherwise, IPv6 uRPF might fail to work.

To enable IPv6 uRPF on an interface:

| Step                                  | Command                                                                                                                 | Remarks                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 1. Enter system view.                 | <b>system-view</b>                                                                                                      | N/A                           |
| 2. Enter interface view.              | <b>interface</b> <i>interface-type</i><br><i>interface-number</i>                                                       | N/A                           |
| 3. Enable IPv6 uRPF on the interface. | <b>ipv6 urpf</b> { <b>loose</b>   <b>strict</b> }<br>[ <b>allow-default-route</b> ] [ <b>acl</b><br><i>acl-number</i> ] | By default, uRPF is disabled. |

## Displaying and maintaining IPv6 uRPF

Execute **display** commands in any view.

| Task                                                                                                      | Command                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display IPv6 uRPF configuration (centralized devices in standalone mode).                                 | <b>display ipv6 urpf</b> [ <b>interface</b> <i>interface-type</i><br><i>interface-number</i> ]                                                                            |
| Display IPv6 uRPF configuration (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display ipv6 urpf</b> [ <b>interface</b> <i>interface-type</i><br><i>interface-number</i> ] [ <b>slot</b> <i>slot-number</i> ]                                         |
| Display IPv6 uRPF configuration (distributed devices in IRF mode).                                        | <b>display ipv6 urpf</b> [ <b>interface</b> <i>interface-type</i><br><i>interface-number</i> ] [ <b>chassis</b> <i>chassis-number</i> <b>slot</b><br><i>slot-number</i> ] |

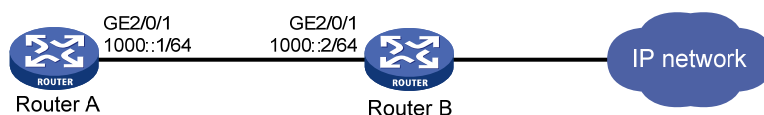
## IPv6 uRPF configuration example

### Network requirements

As shown in [Figure 180](#), configure strict IPv6 uRPF check on GigabitEthernet 2/0/1 of Router B and permit packets from network 1010::/64.

Configure strict IPv6 uRPF check on GigabitEthernet 2/0/1 of Router A and allow using the default route for IPv6 uRPF check.

**Figure 180 Network diagram**



### Configuration procedure

- Configure Router B:
 

```

Define IPv6 ACL 2010 to permit traffic from network 1010::/64.
<RouterB> system-view
[RouterB] acl ipv6 number 2010
[RouterB-acl-basic-2010] rule permit source 1010:: 64
[RouterB-acl-basic-2010] quit

```

```
Specify the IPv6 address of GigabitEthernet 2/0/1.
[RouterB] interface gigabitethernet 2/0/1
[RouterB-GigabitEthernet2/0/1] ipv6 address 1000::2/64
Configure strict uRPF check on GigabitEthernet 2/0/1.
[RouterB-GigabitEthernet2/0/1] ipv6 urpf strict acl 2010
```

**2. Configure Router A:**

```
Specify the IPv6 address of GigabitEthernet 2/0/1.
<RouterA> system-view
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] ipv6 address 1000::1/64
Configure strict uRPF check on GigabitEthernet 2/0/1 and allow using the default route for
IPv6 uRPF check.
[RouterA-GigabitEthernet2/0/1] ipv6 urpf strict allow-default-route
```

# Configuring crypto engines

## Overview

Crypto engines encrypt and decrypt data for service modules. Crypto engines include the following types:

- **Hardware crypto engines**—A hardware crypto engine is a coprocessor integrated on a CPU or hardware crypto card. Hardware crypto engines can accelerate encryption/decryption speed, which improves device processing efficiency. You can enable or disable hardware crypto engines globally as needed.
- **Software crypto engines**—A software crypto engine is a set of software encryption algorithms. The device uses software crypto engines to encrypt and decrypt data for service modules. They are always enabled. You cannot enable or disable software crypto engines.

If you disable hardware crypto engines, the device uses only software crypto engines for data encryption/decryption. If you enable hardware crypto engines, the device preferentially uses hardware crypto engines. If the device does not support hardware crypto engines, or if the hardware crypto engines do not support the required encryption algorithm, the device uses software crypto engines for data encryption/decryption.

Crypto engines provide encryption/decryption services for service modules, for example, the IPsec module. When a service module requires data encryption/decryption, it sends the desired data to a crypto engine. After the crypto engine completes data encryption/decryption, it sends the data back to the service module.

## Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

## Configuring hardware crypto engines

By default, hardware crypto engines are enabled. You can use the **crypto-engine accelerator disable** command to disable them globally. However, disabling hardware crypto engines can degrade the encryption or decryption performance. As a best practice, do not disable hardware crypto engines except for testing, debugging, or troubleshooting purposes.

Enabling or disabling hardware crypto engines affects different service modules differently. For example, for IPsec services, enabling or disabling hardware crypto engines affects only newly established IPsec SAs. The existing IPsec SAs still use the previously selected crypto engine for data encryption. As a best practice, use the **reset ipsec sa** command to delete all existing IPsec SAs before you enable or disable hardware crypto engines.

To configure hardware crypto engines:



| Step                                          | Command                                                                                                                                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                         | <b>system-view</b>                                                                                                                                                                                                               |
| 2. Disable or enable hardware crypto engines. | <ul style="list-style-type: none"> <li>To disable hardware crypto engines:<br/><b>crypto-engine accelerator disable</b></li> <li>To enable hardware crypto engines:<br/><b>undo crypto-engine accelerator disable</b></li> </ul> |

## Displaying and maintaining crypto engines

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                                                                       | Command                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Display crypto engine information.                                                                         | <b>display crypto-engine</b>                                                                                                                      |
| Display crypto engine statistics (centralized devices in standalone mode).                                 | <b>display crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> ]                                                                     |
| Display crypto engine statistics (distributed devices in standalone mode/centralized devices in IRF mode). | <b>display crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> <b>slot</b> <i>slot-number</i> ]                                      |
| Display crypto engine statistics (distributed devices in IRF mode).                                        | <b>display crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ] |
| Clear crypto engine statistics (centralized devices in standalone mode ).                                  | <b>reset crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> ]                                                                       |
| Clear crypto engine statistics (distributed devices in standalone mode/centralized devices in IRF mode).   | <b>reset crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> <b>slot</b> <i>slot-number</i> ]                                        |
| Clear crypto engine statistics (distributed devices in IRF mode).                                          | <b>reset crypto-engine statistics</b> [ <b>engine-id</b> <i>engine-id</i> <b>chassis</b> <i>chassis-number</i> <b>slot</b> <i>slot-number</i> ]   |

# Configuring FIPS

The device that provides low encryption does not support FIPS.

## Overview

Federal Information Processing Standards (FIPS) was developed by the National Institute of Standards and Technology (NIST) of the United States. FIPS specifies the requirements for cryptographic modules. FIPS 140-2 defines four levels of security, named Level 1 to Level 4, from low to high. The device supports Level 2.

Unless otherwise noted, in this document the term FIPS refers to FIPS 140-2.

## Configuration restrictions and guidelines

When you configure FIPS, follow these restrictions and guidelines:

- After the **fips mode enable** command is executed, the system prompts you to choose a reboot method. If you do not make a choice within 30 seconds, the system uses the manual reboot method.
- Before you reboot the device to enter FIPS mode, the system automatically removes all key pairs configured in non-FIPS mode and all FIPS-incompliant digital certificates. FIPS-incompliant digital certificates are MD5-based certificates with the modulus length of key pairs less than 2048 bits. You cannot log in to the device through SSH after the device enters FIPS mode. To log in to the device in FIPS mode through SSH, first log in to the device through a console/AUX/Async port, and then create a key pair for the SSH server.
- The password for entering the device in FIPS mode must comply with the password control policies, such as password length, complexity, and aging policy. When the aging timer for a password expires, the system prompts you to change the password. If you adjust the system time after the device enters FIPS mode, the login password might expire before the next login, because the original system time is typically much earlier than the actual time.
  - If you choose the automatic reboot method, set the system time before executing the **fips mode enable** command.
  - If you choose the manual reboot method, set the system time before configuring the local username and password.
- To use the manual reboot method, you must perform the following tasks:
  - a. Save the current configuration file.
  - b. Specify the current configuration file as the startup configuration file.
  - c. Delete the startup configuration file in binary format.
  - d. Reboot the device.Otherwise, the commands that are not supported by FIPS mode, if they are in the configuration file, might be restored.
- The system enters an intermediate state between when the **fips mode enable** command is executed and when the system is rebooted. If you choose the manual reboot method, do not execute any commands except for the following commands:
  - **reboot**.
  - **save**.
  - Other commands used for configuration preparation to enter FIPS mode.

- Configuration rollback is supported in FIPS mode and also during a switch between FIPS mode and non-FIPS mode. After a configuration rollback between FIPS mode and non-FIPS mode, perform the following tasks:
  - a. Delete the local user and configure a new local user. Local user attributes include password, user role, and service type.
  - b. Save the current configuration file.
  - c. Specify the current configuration file as the startup configuration file.
  - d. Reboot the device. The new configuration takes effect after the reboot. During this process, do not exit the system or perform other operations.
- If a device enters FIPS or non-FIPS mode through automatic reboot, configuration rollback fails. To support configuration rollback, you must execute the **save** command after the device enters FIPS or non-FIPS mode.
- Do not use FIPS and non-FIPS devices to create an IRF fabric.
- To enable FIPS mode for an IRF fabric, you must reboot the entire IRF fabric.

# Configuring FIPS mode

## Entering FIPS mode

After you enable FIPS mode and reboot the device, the device operates in FIPS mode. The FIPS device has strict security requirements, and performs self-tests on cryptography modules to verify that they are operating correctly.

A FIPS device meets the requirements defined in Network Device Protection Profile (NDPP) of Common Criteria (CC).

The system provides two methods to enter FIPS mode: automatic reboot and manual reboot.

### Automatic reboot

To use automatic reboot to enter FIPS mode:

1. Enable FIPS mode.
2. Select the automatic reboot method.

The system automatically performs the following tasks:

- a. Create a default FIPS configuration file named **fips-startup.cfg**.
- b. Specify the default file as the startup configuration file.
- c. Prompt you to configure the username and password for next login.

You can press **Ctrl+C** to exit the configuring process. The **fips mode enable** command will not be executed.

3. Configure a username and password to log in to the device in FIPS mode.

The password must include at least 15 characters that contain uppercase and lowercase letters, digits, and special characters.

The system automatically uses the startup configuration file to reboot the device and enter FIPS mode. You can only use the configured username and password to log in to the FIPS device. After login, you are assigned the role of security administrator Crypto Officer.

### Manual reboot

To use manual reboot to enter FIPS mode:

1. Enable the password control feature globally.
2. Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.

3. Set the minimum length of user passwords to 15 characters.
4. Add a local user account for device management, including the following items:
  - A username.
  - A password that complies with the password control policies as described in step 2 and step 3.
  - A user role of **network-admin**.
  - A service type of **terminal**.
5. Delete the FIPS-incompliant local user service types Telnet, HTTP, and FTP.
6. Enable FIPS mode.
7. Select the manual reboot method.
8. Save the configuration file and specify it as the startup configuration file.
9. Delete the startup configuration file in binary format (an **.mdb** file).
10. Reboot the device.
 

The system enters FIPS mode. You can use the configured username and password to log in to the device in FIPS mode.

To enable FIPS mode:

| Step                  | Command                 | Remarks                                |
|-----------------------|-------------------------|----------------------------------------|
| 1. Enter system view. | <b>system-view</b>      | N/A                                    |
| 2. Enable FIPS mode.  | <b>fips mode enable</b> | By default, the FIPS mode is disabled. |

## Configuration changes in FIPS mode

When the system enters FIPS mode, the following system changes occur:

- The user login authentication mode can only be **scheme**.
- The FTP/TFTP server and client are disabled.
- The Telnet server and client are disabled.
- The HTTP server is disabled.
- SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients and DSA key pairs.
- The generated RSA and DSA key pairs must have a modulus length of 2048 bits.

When the device acts as a server to authenticate a client through the public key, the key pair for the client must also have a modulus length of 2048 bits.

- SSH, SNMPv3, IPsec, and SSL do not support DES, 3DES, RC4, or MD5.
- The password control feature cannot be disabled globally. The **undo password control enable** command does not take effect.
- The keys must contain at least 15 characters and 4 character types of uppercase and lowercase letters, digits, and special characters. This requirement applies to the following passwords:
  - AAA server's shared key.
  - IKE pre-shared key.
  - SNMPv3 authentication key.

The password for a device management local user and password for switching user roles depend on password control policies. By default, the passwords must contain at least 15 characters and 4 character types of uppercase and lowercase letters, digits, and special characters.

## Exiting FIPS mode

After you disable FIPS mode and reboot the device, the device operates in non-FIPS mode.

The system provides two methods to exit FIPS mode: automatic reboot and manual reboot.

### Automatic reboot

Select the automatic reboot method. The system automatically creates a default non-FIPS configuration file named **non-fips-startup.cfg**, and specifies the file as the startup configuration file. The system reboots the device by using the default non-FIPS configuration file. After the reboot, you are directly logged into the device.

### Manual reboot

This method requires that you manually complete the configurations for entering non-FIPS mode, and then reboot the device. To log in to the device after the reboot, you must enter user information according to the authentication mode. The following default authentication modes are available for different ports or lines (you can modify the default mode as needed):

- The default authentication mode is **password** for VTY lines.
- If the device has both a console port and an AUX port, the default authentication mode is **none** for the console port, and is **password** for the AUX port.
- If the device supports either a console port or an AUX port, the default authentication mode is **none** for the console or AUX port.

After you disable FIPS mode, follow these restrictions and guidelines before you manually reboot the device:

- If you are logged into the device through Telnet, perform the following tasks without exiting the current user line:
  - Set the authentication mode to **scheme**.
  - Configure the username and password. (You can also use the current username and password.)
- If you are logged into the device through a console/AUX/Async port, configure one of the following authentication modes as needed:
  - Configure the **password** authentication mode and a password.
  - Configure the **scheme** authentication mode and configure a new username and password (you can also use the current username and password).
  - Configure the **none** authentication mode.

To disable FIPS mode:

| Step                  | Command                      | Remarks                                |
|-----------------------|------------------------------|----------------------------------------|
| 1. Enter system view. | <b>system-view</b>           | N/A                                    |
| 2. Disable FIPS mode. | <b>undo fips mode enable</b> | By default, the FIPS mode is disabled. |

# FIPS self-tests

To ensure the correct operation of cryptography modules, FIPS provides self-test mechanisms, including power-up self-test and conditional self-test. You can also trigger a self-test. If the power-up self-test fails, the card where the self-test process exists reboots. If the conditional self-test fails, the system outputs self-test failure information.

---

**NOTE:**

If a self-test fails, contact Hewlett Packard Enterprise Support.

---

## Power-up self-tests

The power-up self-test, also called known-answer test, examines the availability of FIPS-allowed cryptographic algorithms. A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the known-answer test fails.

The power-up self-test examines the cryptographic algorithms listed in [Table 15](#).

**Table 15 Power-up self-test list**

| Type                              | Operations                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cryptographic algorithm self-test | Tests the following algorithms: <ul style="list-style-type: none"><li>• DSA (signature and authentication).</li><li>• RSA (signature and authentication).</li><li>• RSA (encryption and decryption).</li><li>• AES.</li><li>• 3DES.</li><li>• SHA1.</li><li>• HMAC-SHA1.</li><li>• Random number generator algorithms.</li></ul>                               |
| Cryptographic engine self-test    | Tests the following algorithms used by cryptographic engines: <ul style="list-style-type: none"><li>• DSA (signature and authentication).</li><li>• RSA (signature and authentication).</li><li>• RSA (encryption and decryption).</li><li>• AES.</li><li>• 3DES.</li><li>• SHA1.</li><li>• HMAC-SHA1.</li><li>• Random number generator algorithms.</li></ul> |

## Conditional self-tests

A conditional self-test runs when an asymmetrical cryptographic module or a random number generator module is invoked. Conditional self-tests include the following types:

- **Pair-wise consistency test**—This test is run when a DSA/RSA asymmetrical key-pair is generated. It uses the public key to encrypt a plain text, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.
- **Continuous random number generator test**—This test is run when a random number is generated. Each subsequent generation of a random number will be compared with the

previously generated number. The test fails if any two compared numbers are the same. This test can also be run when a DSA/RSA asymmetrical key-pair is generated.

## Triggering self-tests

To examine whether the cryptography modules operate correctly, you can trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test. If the self-test fails, the card where the self-test process exists reboots.

To trigger a self-test:

| Step                    | Command               |
|-------------------------|-----------------------|
| 1. Enter system view.   | <b>system-view</b>    |
| 2. Trigger a self-test. | <b>fips self-test</b> |

## Displaying and maintaining FIPS

Execute **display** commands in any view.

| Task                         | Command                    |
|------------------------------|----------------------------|
| Display the FIPS mode state. | <b>display fips status</b> |

## FIPS configuration examples

### Entering FIPS mode through automatic reboot

#### Network requirements

Use the automatic reboot method to enter FIPS mode, and use a console/AUX/Async port to log in to the device in FIPS mode.

#### Configuration procedure

# If you want to save the current configuration, execute the **save** command before you enable FIPS mode.

# Enable FIPS mode and choose the automatic reboot method to enter FIPS mode. Set the username to **root** and the password to **12345zxcvb!@#\$%ZXCVB**.

```
<Sysname> system-view
```

```
[Sysname] fips mode enable
```

```
FIPS mode change requires a device reboot. Continue? [Y/N]:y
```

```
Reboot the device automatically? [Y/N]:y
```

The system will create a new startup configuration file for FIPS mode. After you set the login username and password for FIPS mode, the device will reboot automatically.

```
Enter username(1-55 characters):root
```

```
Enter password(15-63 characters):
```

```
Confirm password:
```

```
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

## Verifying the configuration

After the device reboots, enter the username **root** and the password **12345zxcvb!@#\$%ZXCVB**. The system prompts you to configure a new password. After you configure the new password, the device enters FIPS mode. The new password must be different from the previous password. It must include at least 15 characters, and contain uppercase and lowercase letters, digits, and special characters. For more information about the requirements for the password, see the system output.

Press ENTER to get started.

login: root

Password:

First login or password reset. For security reason, you need to change your password. Please enter your password.

old password:

new password:

confirm:

Updating user information. Please wait ... ..

...

<Sysname>

# Display the current FIPS mode state.

<Sysname> display fips status

FIPS mode is enabled.

# Display the default configuration file.

<Sysname> more fips-startup.cfg

#

password-control enable

#

local-user root class manage

service-type terminal

authorization-attribute user-role network-admin

#

fips mode enable

#

return

<Sysname>

## Entering FIPS mode through manual reboot

### Network requirements

Use the manual reboot method to enter FIPS mode, and use a console/AUX/Async port to log in to the device in FIPS mode.

### Configuration procedure

# Enable the password control feature globally.

<Sysname> system-view

[Sysname] password-control enable

# Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.

[Sysname] password-control composition type-number 4 type-length 1



```

Set the minimum length of user passwords to 15 characters.
[Sysname] password-control length 15

Add a local user account for device management, including a username of test, a password of
12345zxcvb!@#$$%ZXCVB, a user role of network-admin, and a service type of terminal.
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 12345zxcvb!@#$$%ZXCVB
[Sysname-luser-manage-test] authorization-attribute user-role network-admin
[Sysname-luser-manage-test] service-type terminal
[Sysname-luser-manage-test] quit

Enable FIPS mode, and choose the manual reboot method to enter FIPS mode.
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.

Save the current configuration to the root directory of the storage medium, and specify it as the
startup configuration file.
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit

Delete the startup configuration file in binary format.
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.

Reboot the device.
<Sysname> reboot

```

## Verifying the configuration

After the device reboots, enter the username **test** and the password **12345zxcvb!@#\$\$%ZXCVB**. The system prompts you to configure a new password. After you configure the new password, the device enters FIPS mode. The new password must be different from the previous password. It must include at least 15 characters, and contain uppercase and lowercase letters, digits, and special characters. For more information about the requirements for the password, see the system output. Press ENTER to get started.

```

login: test
Password:
First login or password reset. For security reason, you need to change your pass
word. Please enter your password.
old password:
new password:
confirm:
Updating user information. Please wait
...
<Sysname>

```

```
Display the current FIPS mode state.
<Sysname> display fips status
FIPS mode is enabled.
```

## Exiting FIPS mode through automatic reboot

### Network requirements

A user has logged in to the device in FIPS mode through a console/AUX/Async port.  
Use the automatic reboot method to exit FIPS mode.

### Configuration procedure

```
Disable FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot
automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

### Verifying the configuration

After the device reboots, you can enter the system.  
<Sysname>  
  
# Display the current FIPS mode state.  
<Sysname> display fips status  
FIPS mode is disabled.

## Exiting FIPS mode through manual reboot

### Network requirements

A user has logged in to the device in FIPS mode through SSH with the username **test** and password **12345zxcvb!@#\$%ZXCVB**.  
Use the manual reboot method to exit FIPS mode.

### Configuration procedure

```
Disable FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot
automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to
the next-startup configuration file, and then reboot to enter non-FIPS mode.

Set the authentication mode for VTY lines to scheme.
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme

Save the current configuration to the root directory of the storage medium, and specify it as the
startup configuration file.
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
```

```
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit

Delete the startup configuration file in binary format.
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.

Reboot the device.
<Sysname> reboot
```

## Verifying the configuration

After the device reboots, enter the username **test** and password **12345zxcvb!@#%ZXCVB** to enter non-FIPS mode.

Press ENTER to get started.

```
login: test
Password:
Last successfully login time:...
...
<Sysname>

Display the current FIPS mode state.
<Sysname> display fips status
FIPS mode is disabled.
```

# Configuring mGRE

## Overview

Multipoint Generic Routing Encapsulation (mGRE) is a dynamic VPN technology that uses the Next Hop Resolution Protocol (NHRP).

Traditional GRE tunnels for a VPN are static and require manual configuration and maintenance, resulting in poor extensibility. If branches of an enterprise access the public network by using dynamic IP addresses, it is difficult to set GRE tunnels between the branches.

mGRE can dynamically establish tunnels for the branches, because NHRP can map the private IP address of a branch to its public IP address.

## mGRE operation scheme

An mGRE network uses the client/server model. It has the following types of nodes:

- **NHS**—NHRP server, the hub device in the mGRE network. The NHS is the routing information exchange center. It is also the data forwarding center in a NHS-NHC network.
- **NHC**—NHRP client, a spoke device in the mGRE network. Typically, it is the gateway of a branch network. An NHC does not forward data received from other mGRE nodes.

mGRE obtains dynamic public addresses of NHCs through their private addresses to establish mGRE tunnels and forward packets. The public address is the IP address of the interface connected to the Internet. The private address is the IP address of the mGRE tunnel interface.

An NHC registers its public and private addresses with the NHS and it registers its public address whenever the public address changes. An NHC obtains the current public address of a peer NHC from the NHS through NHRP, so the two NHCs can establish an mGRE tunnel over the Internet.

## mGRE operation procedure

The mGRE operation includes the following phases:

- Registration.
- Tunnel establishment.
- Route learning and packet forwarding.

### Registration

As shown in [Figure 181](#), the registration process is as follows:

1. The NHC sends a registration request to the NHS.
2. After the NHS receives the request, it performs the NHRP packet authentication key and GRE key matching. If both keys are matched, registration succeeds. The NHS sends a registration success message to the NHC.

**Figure 181 Registration process**

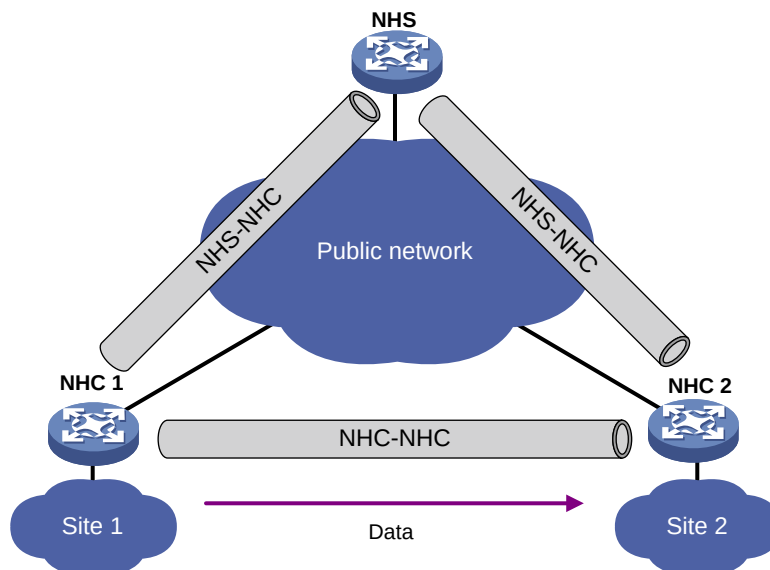


## Tunnel establishment

mGRE networks support the following types of networking:

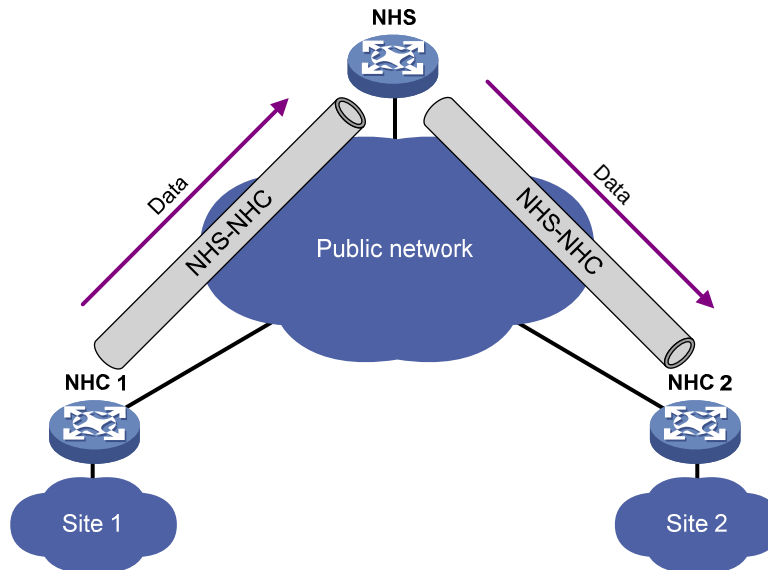
- **Full-mesh network**—NHCs can establish tunnels between each other for direct communication. The NHS acts as the routing information exchange center.

**Figure 182 Full-mesh network**



- **NHS-NHC network**—NHCs cannot establish tunnels between each other. Instead, they establish tunnels with the NHS. The NHS forwards data for the NHCs. The NHS acts as both the routing information exchange center and the data forwarding center.

**Figure 183 NHS-NHC network**



A mGRE tunnel is as established as follows:

- **NHC-NHS tunnel establishment process:**  
An NHC-NHS tunnel is established in the registration process. During registration, the NHC-NHS tunnel is in initialization state. After registration succeeds, the NHC-NHS tunnel is in success state.  
An NHC-NHS tunnel is permanent. An NHC can establish permanent tunnels to any number of NHSs.
- **NHC-NHC tunnel establishment process:**
  - a. In a full-mesh network, when an NHC receives a data packet but finds no tunnel for forwarding the packet, the NHC (initiator) sends an address resolution request to the NHS.
  - b. After receiving the request, the NHS looks up the local NHRP mapping table to find the peer NHC (responder) and forwards the request to the peer NHC.
  - c. After receiving the request, the peer NHC creates a temporary tunnel and sends an address resolution response to the initiator.An NHC-NHC tunnel is dynamic. If no data is exchanged within the NHC-NHC tunnel idle timeout, the tunnel will be deleted.

## **Route learning and packet forwarding**

mGRE nodes learn private routes by using dynamic routing protocols.

Dynamic routing must be configured for all private networks and mGRE tunnel interfaces to ensure IP connectivity among the private networks. From the perspective of private networks, an mGRE tunnel is a link that connects different private networks. A dynamic routing protocol discovers neighbors and updates routes over mGRE tunnels, and establishes a routing table.

When an NHC receives a packet destined for a remote private network, it performs the following operations:

1. Searches the routing table for the next hop address to the target private network.
2. Looks up the local NHRP mapping table to obtain the public address that corresponds to the next hop address.
3. Uses the public address as the tunnel destination address to encapsulate the packet.
4. Sends the encapsulated packet to the peer NHC over the mGRE tunnel.

# mGRE support for NAT traversal

An NHC-NHC tunnel can traverse a NAT gateway. The tunnel can be established when the tunnel initiator, receiver, or both ends reside behind the NAT gateway.

## mGRE configuration task list

To set up an mGRE network, first configure the NHSs and then the NHCs.



### IMPORTANT:

The device can act only as an NHC. It cannot act as an NHS.

To configure mGRE on an NHC:

| Tasks at a glance                                                |
|------------------------------------------------------------------|
| (Required.)<br>Configuring an mGRE tunnel                        |
| (Required.) Configuring routing                                  |
| (Optional.) <a href="#">Configuring IPsec for an mGRE tunnel</a> |

## Configuring an mGRE tunnel

The public address of an NHC can be statically configured or dynamically assigned. The private address of an NHC must be statically configured.

For more information about tunnel interfaces, see tunneling configuration in *Layer 3—IP Services Configuration Guide*. For more information about the **interface tunnel**, **source**, and **tunnel dfbit enable** commands and other commands for a tunnel interface, see tunneling commands in *Layer 3—IP Services Command Reference*.

To configure an mGRE tunnel:

| Step                                                                        | Command                                                                                 | Remarks                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Enter system view.                                                       | <b>system-view</b>                                                                      | N/A                                                                                                                                                                                                                                                                                                                               |
| 2. Create an mGRE tunnel interface and enter tunnel interface view.         | <b>interface tunnel</b> <i>number</i><br><b>mode mgre</b>                               | By default, no tunnel interfaces exist.                                                                                                                                                                                                                                                                                           |
| 3. Configure a private address for the tunnel interface.                    | <b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> } [ <b>sub</b> ] | By default, no private address is configured for a tunnel interface.                                                                                                                                                                                                                                                              |
| 4. Configure a source address or source interface for the tunnel interface. | <b>source</b> { <i>ip-address</i>   <i>interface-type</i> <i>interface-number</i> }     | By default, no source address or source interface is configured for a tunnel interface.<br><br>If you specify a source address, it is used as the source IP address of tunneled packets.<br><br>If you specify a source interface, the primary IP address of this interface is used as the source IP address of tunneled packets. |

| Step                                                         | Command                                                                    | Remarks                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Configure an NHRP packet authentication key.              | <b>nhrp authentication</b> [ <b>cipher</b>   <b>simple</b> ] <i>string</i> | By default, no NHRP packet authentication key is configured. NHRP nodes do not authenticate NHRP packets received from each other.                                                                                                                                                                                                                                                                       |
| 6. Configure an NHRP network ID for the mGRE tunnel.         | <b>nhrp network-id</b> <i>number</i>                                       | By default, an mGRE tunnel does not have an NHRP network ID.                                                                                                                                                                                                                                                                                                                                             |
| 7. Configure the holdtime for NHRP mapping entries.          | <b>nhrp holdtime</b> <i>seconds</i>                                        | By default, the holdtime of NHRP mapping entries is 7200 seconds.                                                                                                                                                                                                                                                                                                                                        |
| 8. Configure an NHS private-to-public address mapping.       | <b>nhrp nhs</b> <i>nhs-address nbma nbma-address</i>                       | By default, no NHS private-to-public address mappings are configured.                                                                                                                                                                                                                                                                                                                                    |
| 9. (Optional.) Configure a GRE key for the tunnel interface. | <b>gre key</b> <i>key</i>                                                  | By default, no GRE key is configured for an mGRE tunnel interface.<br>You must configure the same GRE key or configure no key on both ends of a tunnel.<br>On the device, you must configure different GRE keys for mGRE tunnel interfaces that have the same source address or source interface.<br>For more information about the GRE key, see GRE in <i>Layer 3—IP Services Configuration Guide</i> . |
| 10. (Optional.) Set the DF bit for tunneled packets.         | <b>tunnel dfbit enable</b>                                                 | By default, the DF bit is not set. Tunneled packets can be fragmented for forwarding.                                                                                                                                                                                                                                                                                                                    |

## Configuring routing

mGRE clients support dynamic routing protocols of OSPF, RIP, and BGP.

When you configure routing for mGRE client, following these restrictions and guidelines:

- When OSPF is used, specify the OSPF interface network type as **broadcast** in a full-mesh network and as **p2mp** in a NHS-NHC network.
- Full-mesh networks do not support RIP. NHS-NHC networks must use the RIP-2 multicast mode and disable the split horizon feature for NHS nodes.
- When BGP is used, configure routing policies to ensure the following:
  - In a full-mesh network, ensure that the local NHC learns a route to the remote private network, and the route's next hop address is the address of the remote NHC.
  - In an NHS-NHC network, ensure that the local NHC learns a route to the remote private network, and the route's next hop address is the address of the NHS.

For more information about OSPF, RIP, BGP, and routing policy configuration, see *Layer 3—IP Routing Configuration Guide*.

## Configuring IPsec for an mGRE tunnel

The device supports protecting mGRE tunnel data and control packets by using IPsec profiles.

To configure IPsec for an mGRE tunnel:



1. Configure an IPsec transform set to specify the security protocol, authentication and encryption algorithms, and encapsulation type.
2. Configure an IKE-based IPsec profile.
3. Apply the IKE-based IPsec profile to the mGRE tunnel interface.

For more information about IPsec configuration, see "Configuring IPsec."

## Displaying and maintaining mGRE

Execute **display** commands in any view and **reset** commands in user view.

| Task                                                  | Command                                                                                                                                |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Display information about NHRP mapping entries.       | <b>display nhrp map</b> [ <b>interface tunnel</b> <i>interface-number</i> [ <b>peer</b> <i>ipv4-address</i> ] ] [ <b>verbose</b> ]     |
| Display NHRP packet statistics for tunnel interfaces. | <b>display nhrp statistics</b> [ <b>interface tunnel</b> <i>interface-number</i> ]                                                     |
| Display mGRE session information.                     | <b>display mgre session</b> [ <b>interface tunnel</b> <i>interface-number</i> [ <b>peer</b> <i>ipv4-address</i> ] ] [ <b>verbose</b> ] |
| Clear NHRP packet statistics for tunnel interfaces.   | <b>reset nhrp statistics</b> [ <b>interface tunnel</b> <i>interface-number</i> ]                                                       |
| Reset mGRE sessions.                                  | <b>reset mgre session</b> [ <b>interface tunnel</b> <i>interface-number</i> [ <b>peer</b> <i>ipv4-address</i> ] ]                      |
| Clear mGRE session statistics.                        | <b>reset mgre statistics</b> [ <b>interface tunnel</b> <i>interface-number</i> [ <b>peer</b> <i>ipv4-address</i> ] ]                   |

## mGRE configuration examples

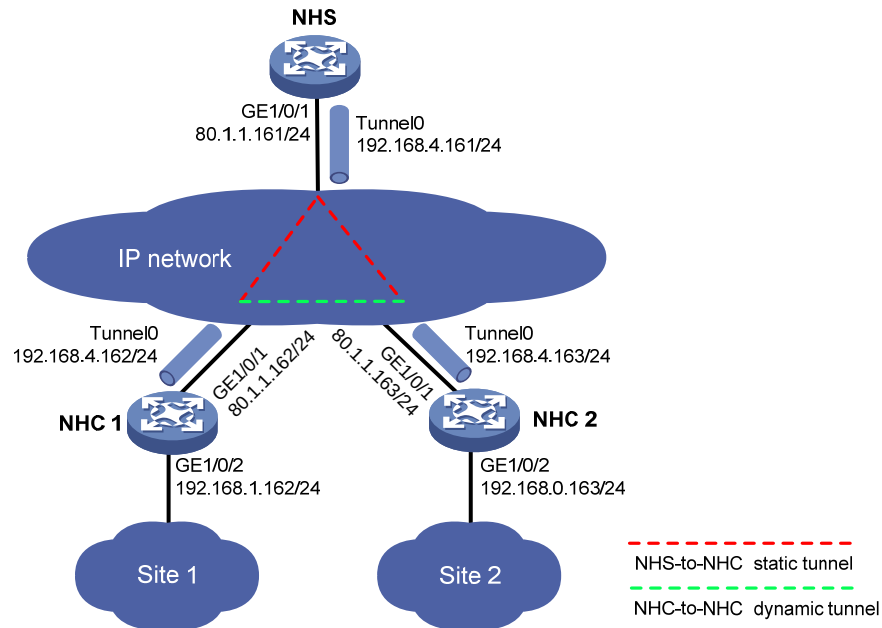
### Full-mesh mGRE network configuration example

#### Network requirements

As shown in [Figure 184](#), construct a full-mesh mGRE network. The NHS manages and maintains information for each node.

Set up permanent (static) mGRE tunnels between the NHS and NHCs. Set up temporary (dynamic) mGRE tunnels between NHCs when they need to communicate with each other.

**Figure 184 Network diagram**



## Configuration procedure

### 1. Configure NHC 1:

```
Configure an IP address for GigabitEthernet 1/0/1.
<NHC1> system-view
[NHC1] interface gigabitethernet 1/0/1
[NHC1-GigabitEthernet1/0/1] ip address 80.1.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC1] interface gigabitethernet 1/0/2
[NHC1-GigabitEthernet1/0/2] ip address 192.168.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] ip address 192.168.4.162 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC1-Tunnel0] ospf network-type broadcast
Enable OSPF for the tunnel interface.
[NHC1-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC1-Tunnel0] source gigabitethernet1/0/1
Set the GRE key to 100000.
[NHC1-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC1-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC1-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
```

```

[NHC1-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC1-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC1-Tunnel0] quit
Configure basic OSPF.
[NHC1] ospf 1
[NHC1-ospf-1] area 0.0.0.1
[NHC1-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] quit

```

## 2. Configure NHC 2:

```

Configure an IP address for GigabitEthernet 1/0/1.
<NHC2> system-view
[NHC2] interface gigabitethernet 1/0/1
[NHC2-GigabitEthernet1/0/1] ip address 80.1.1.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC2] interface gigabitethernet 1/0/2
[NHC2-GigabitEthernet1/0/2] ip address 192.168.0.163 255.255.255.0
[NHC2-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] ip address 192.168.4.163 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC2-Tunnel0] ospf network-type broadcast
Enable OSPF for the tunnel interface.
[NHC2-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC2-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC2-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC2-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC2-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
[NHC2-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC2-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC2-Tunnel0] quit
Configure basic OSPF.
[NHC2] ospf 1
[NHC2-ospf-1] area 0.0.0.1
[NHC2-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] network 192.168.0.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] quit

```

## Verifying the configuration

# Display detailed information about the NHRP table on NHC 1.

```
[NHC1] display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 00:11:21
Expiration time : never expire
Type : static
Flags : up
NBMA address : 80.1.1.161
```

# Display brief information about the NHRP session on NHC 1.

```
[NHC1] display mgre session
Interface : Tunnel0
Number of sessions: 1
Peer NBMA address Peer protocol address Type State State duration
80.1.1.161 192.168.4.161 C-S Succeeded 00:09:42
```

The output indicates that NHC 1 has established a permanent tunnel with the NHS. The output on NHC 2 is similar.

# Ping the private address 192.168.4.163 of NHC 2 from NHC 1.

```
[NHC1] ping 192.168.4.163
Ping 192.168.4.163 (192.168.4.163): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.4.163: icmp_seq=0 ttl=255 time=3.314 ms
56 bytes from 192.168.4.163: icmp_seq=1 ttl=255 time=2.786 ms
56 bytes from 192.168.4.163: icmp_seq=2 ttl=255 time=2.317 ms
56 bytes from 192.168.4.163: icmp_seq=3 ttl=255 time=3.060 ms
56 bytes from 192.168.4.163: icmp_seq=4 ttl=255 time=2.258 ms
```

--- Ping statistics for 192.168.4.163 ---

5 packets transmitted, 5 packets received, 0.0% packet loss  
round-trip min/avg/max/std-dev = 2.258/2.747/3.314/0.411 ms

# Display detailed information about the NHRP table on NHC 1.

```
[NHC1] display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 01:10:25
Expiration time : never expire
Type : static
Flags : up
NBMA address : 80.1.1.161
```

```
Interface : Tunnel0
Destination/mask : 192.168.4.163/32
Next hop : 192.168.4.163
Creation time : 00:00:24
Expiration time : 00:01:36
```

```
Type : cached
Flags : used up
NBMA address : 80.1.1.163
```

# Display brief information about the NHRP session on NHC 1.

```
[NHC1] display mgre session
```

```
Interface : Tunnel0
```

```
Number of sessions: 2
```

| Peer NBMA address | Peer protocol address | Type | State     | State duration |
|-------------------|-----------------------|------|-----------|----------------|
| 80.1.1.161        | 192.168.4.161         | C-S  | Succeeded | 00:10:28       |
| 80.1.1.163        | 192.168.4.163         | C-C  | Succeeded | 00:00:32       |

The output indicates that NHC 1 has established a permanent tunnel with the NHS and a temporary tunnel with NHC 2. The output on NHC 2 is similar.

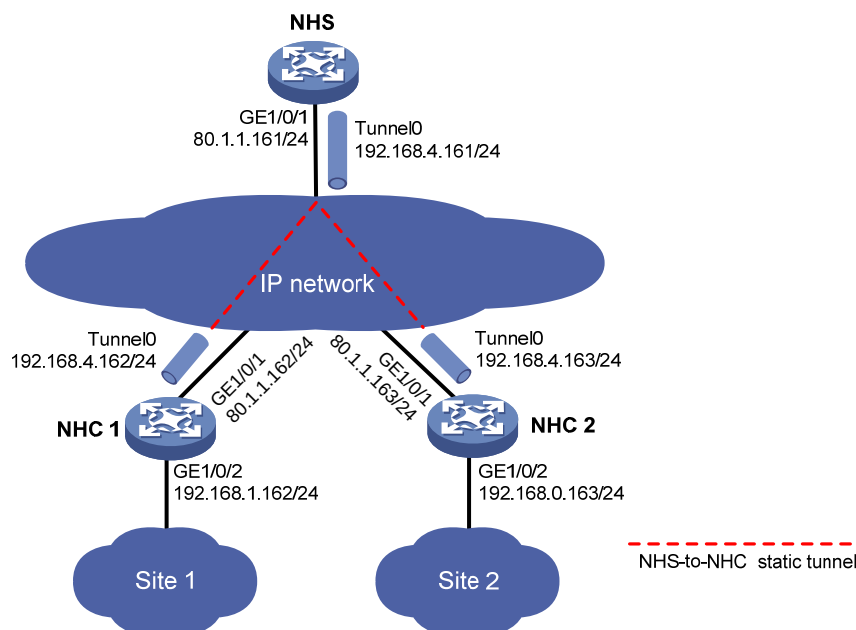
## NHS-NHC mGRE network configuration example

### Network requirements

As shown in Figure 185, construct an NHS-NHC mGRE network. The NHS manages and maintains information for each node and forwards packets between NHCs.

Set up permanent (static) mGRE tunnels between the NHS and NHCs.

**Figure 185 Network diagram**



### Configuration procedure

#### 1. Configure NHC 1:

# Configure an IP address for GigabitEthernet 1/0/1.

```
<NHC1> system-view
```

```
[NHC1] interface gigabitethernet 1/0/1
```

```
[NHC1-GigabitEthernet1/0/1] ip address 80.1.1.162 255.255.255.0
```

```
[NHC1-GigabitEthernet1/0/1] quit
```

# Configure an IP address for GigabitEthernet 1/0/2.

```

[NHC1] interface gigabitethernet 1/0/2
[NHC1-GigabitEthernet1/0/2] ip address 192.168.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] ip address 192.168.4.162 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC1-Tunnel0] ospf network-type p2mp
Enable OSPF for the tunnel interface.
[NHC1-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC1-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC1-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC1-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC1-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
[NHC1-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC1-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC1-Tunnel0] quit
Configure basic OSPF.
[NHC1] ospf 1
[NHC1-ospf-1] area 0.0.0.1
[NHC1-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] quit

```

## 2. Configure NHC 2:

```

Configure an IP address for GigabitEthernet 1/0/1.
<NHC2> system-view
[NHC2] interface gigabitethernet1/0/1
[NHC2-GigabitEthernet1/0/1] ip address 80.1.1.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC2] interface gigabitethernet1/0/2
[NHC2-GigabitEthernet1/0/2] ip address 192.168.0.163 255.255.255.0
[NHC2-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] ip address 192.168.4.163 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC2-Tunnel0] ospf network-type p2mp
Enable OSPF for the tunnel interface.
[NHC2-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.

```

```

[NHC2-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC2-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC2-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC2-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
[NHC2-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC2-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC2-Tunnel0] quit
Configure basic OSPF.
[NHC2] ospf 1
[NHC2-ospf-1] area 0.0.0.1
[NHC2-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] network 192.168.0.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] quit

```

## Verifying the configuration

# Display detailed information about the NHRP table on NHC 1.

```

[NHC1] display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 07:50:32
Expiration time : never expire
Type : static
Flags : up
NBMA address : 80.1.1.161

```

# Display brief information about the NHRP session on NHC 1.

```

[NHC1] display mgre session
Interface : Tunnel0
Number of sessions: 1
Peer NBMA address Peer protocol address Type State State duration
80.1.1.161 192.168.4.161 C-S Succeeded 07:49:14

```

The output indicates that NHC 1 has established a permanent tunnel with the NHS. The output on NHC 2 is similar.

# On NHC 1, test the connectivity between Site 1 and Site 2. The ping operation succeeds.

```

[NHC1] ping -a 192.168.1.162 192.168.0.163
Ping 192.168.0.163 (192.168.0.163) from 192.168.1.162: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.163: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 192.168.0.163: icmp_seq=1 ttl=254 time=17.000 ms
56 bytes from 192.168.0.163: icmp_seq=2 ttl=254 time=14.000 ms
56 bytes from 192.168.0.163: icmp_seq=3 ttl=254 time=7.000 ms
56 bytes from 192.168.0.163: icmp_seq=4 ttl=254 time=7.000 ms

```

```

--- Ping statistics for 192.168.0.163 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 7.000/11.000/17.000/3.950 ms

```

## IPsec-protected full-mesh mGRE network configuration example

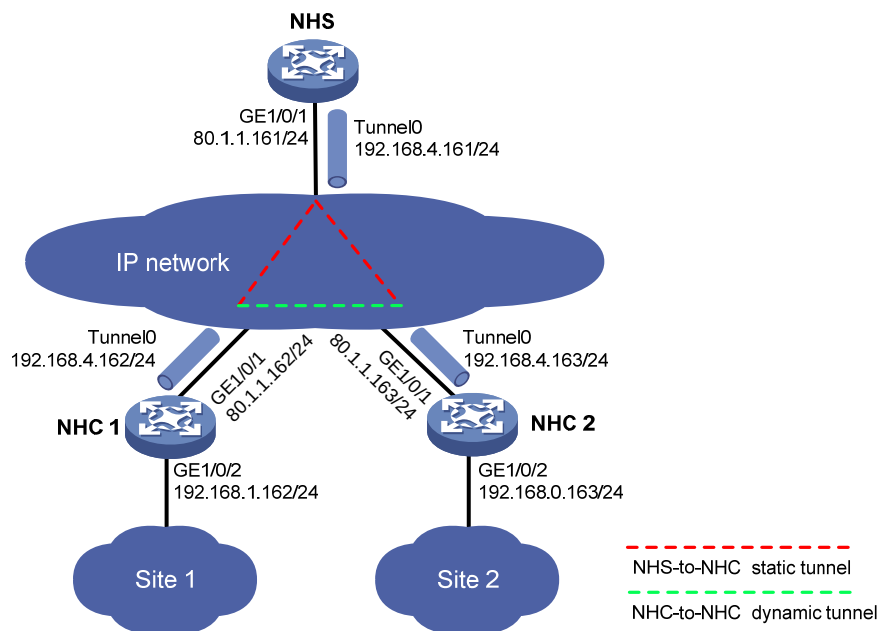
### Network requirements

As shown in [Figure 186](#), construct a full-mesh mGRE network. The NHS manages and maintains information for each node.

Set up permanent (static) mGRE tunnels between the NHS and NHCs. Set up temporary (dynamic) mGRE tunnels between NHCs when they need to communicate with each other.

Configure IPsec to protect the mGRE tunnels.

**Figure 186 Network diagram**



### Configuration procedure

#### 1. Configure NHC 1:

```

Configure an IP address for GigabitEthernet 1/0/1.
<NHC1> system-view
[NHC1] interface gigabitethernet 1/0/1
[NHC1-GigabitEthernet1/0/1] ip address 80.1.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC1] interface gigabitethernet 1/0/2
[NHC1-GigabitEthernet1/0/2] ip address 192.168.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] ip address 192.168.4.162 255.255.255.0

```



```

Specify the OSPF interface network type as broadcast.
[NHC1-Tunnel0] ospf network-type broadcast

Enable OSPF for the tunnel interface.
[NHC1-Tunnel0] ospf 1 area 0.0.0.1

Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC1-Tunnel0] source gigabitethernet 1/0/1

Set the GRE key to 100000.
[NHC1-Tunnel0] gre key 100000

Set the NHRP network ID to 9.
[NHC1-Tunnel0] nhrp network-id 9

Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC1-Tunnel0] nhrp authentication simple 12345678

Set the holdtime of NHRP mapping entries to 3600 seconds.
[NHC1-Tunnel0] nhrp holdtime 3600

Configure an NHS private-to-public address mapping.
[NHC1-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC1-Tunnel0] quit

Configure basic OSPF.
[NHC1] ospf 1
[NHC1-ospf-1] area 0.0.0.1
[NHC1-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] quit

Configure an IPsec transform set named aa. Specify the encryption algorithm as 56-bit DES
and authentication algorithm as HMAC-SHA1.
[NHC1] ipsec transform-set aa
[NHC1-ipsec-transform-set-aa] esp encryption-algorithm des-cbc
[NHC1-ipsec-transform-set-aa] esp authentication-algorithm sha1
[NHC1-ipsec-transform-set-aa] quit

Create IKE keychain 1.
[NHC1] ike keychain 1

Configure the pre-shared key used with the peer 80.1.1.161 as a plaintext string of 12345678.
[NHC1-ike-keychain-1] pre-shared-key address 80.1.1.161 24 key simple 12345678
[NHC1-ike-keychain-1] quit

Create an IKE profile named abc.
[NHC1] ike profile abc

Specify IKE keychain 1 for the IKE profile.
[NHC1-ike-profile-abc] keychain 1
[NHC1-ike-profile-abc] quit

Create an IKE-based IPsec profile named abc.
[NHC1] ipsec profile abc isakmp

Specify IPsec transform set aa for the IPsec profile.
[NHC1-ipsec-profile-isakmp-abc] transform-set aa

Specify IKE profile abc for the IPsec profile.
[NHC1-ipsec-profile-isakmp-abc] ike-profile abc
[NHC1-ipsec-profile-isakmp-abc] quit

Apply IPsec profile abc to the mGRE tunnel interface.

```

```
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] tunnel protection ipsec profile abc
[NHC1-Tunnel0] quit
```

## 2. Configure NHC 2:

# Configure an IP address for GigabitEthernet 1/0/1.

```
<NHC2> system-view
[NHC2] interface gigabitethernet 1/0/1
[NHC2-GigabitEthernet1/0/1] ip address 80.1.1.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit
```

# Configure an IP address for GigabitEthernet 1/0/2.

```
[NHC2] interface gigabitethernet 1/0/2
[NHC2-GigabitEthernet1/0/2] ip address 192.168.0.163 255.255.255.0
[NHC2-GigabitEthernet1/0/2] quit
```

# Configure an IP address for mGRE tunnel interface Tunnel0.

```
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] ip address 192.168.4.163 255.255.255.0
```

# Specify the OSPF interface network type as broadcast.

```
[NHC2-Tunnel0] ospf network-type broadcast
```

# Enable OSPF for the tunnel interface.

```
[NHC2-Tunnel0] ospf 1 area 0.0.0.1
```

# Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.

```
[NHC2-Tunnel0] source gigabitethernet 1/0/1
```

# Set the GRE key to 100000.

```
[NHC2-Tunnel0] gre key 100000
```

# Set the NHRP network ID to 9.

```
[NHC2-Tunnel0] nhrp network-id 9
```

# Configure the NHRP packet authentication key as a plaintext string of 123456.

```
[NHC2-Tunnel0] nhrp authentication simple 12345678
```

# Set the holdtime of NHRP mapping entries to 3600 seconds.

```
[NHC2-Tunnel0] nhrp holdtime 3600
```

# Configure an NHS private-to-public address mapping.

```
[NHC2-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
```

```
[NHC2-Tunnel0] quit
```

# Configure basic OSPF.

```
[NHC2] ospf 1
[NHC2-ospf-1] area 0.0.0.1
[NHC2-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] network 192.168.0.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] quit
```

# Configure an IPsec transform set named **aa**. Specify the encryption algorithm as 56-bit DES and authentication algorithm as HMAC-SHA1.

```
[NHC2] ipsec transform-set aa
[NHC2-ipsec-transform-set-aa] esp encryption-algorithm des-cbc
[NHC2-ipsec-transform-set-aa] esp authentication-algorithm sha1
[NHC2-ipsec-transform-set-aa] quit
```

# Create IKE keychain 1.

```
[NHC2] ike keychain 1
```

```

Configure the pre-shared key used with the peer 80.1.1.161 as a plaintext string of 12345678.
[NHC2-ike-keychain-1] pre-shared-key address 80.1.1.161 24 key simple 12345678
[NHC2-ike-keychain-1] quit
Create an IKE profile named abc.
[NHC2] ike profile abc
Specify IKE keychain 1 for the IKE profile.
[NHC2-ike-profile-abc] keychain 1
[NHC2-ike-profile-abc] quit
Create an IKE-based IPsec profile named abc.
[NHC2] ipsec profile abc isakmp
Specify IPsec transform set aa for the IPsec profile.
[NHC2-ipsec-profile-isakmp-abc] transform-set aa
Specify IKE profile abc for the IPsec profile.
[NHC2-ipsec-profile-isakmp-abc] ike-profile abc
[NHC2-ipsec-profile-isakmp-abc] quit
Apply IPsec profile abc to the mGRE tunnel interface.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] tunnel protection ipsec profile abc
[NHC2-Tunnel0] quit

```

## Verifying the configuration

# Display detailed information about the NHRP table on NHC 1.

```

[NHC1] display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 00:30:51
Expiration time : never expire
Type : static
Flags : up ipsec
NBMA address : 80.1.1.161

```

# Display brief information about the NHRP session on NHC 1.

```

[NHC1] display mgre session
Interface : Tunnel0
Number of sessions: 1

```

| Peer NBMA address | Peer protocol address | Type | State     | State duration |
|-------------------|-----------------------|------|-----------|----------------|
| 80.1.1.161        | 192.168.4.161         | C-S  | Succeeded | 00:09:42       |

The output indicates that NHC 1 has established a permanent tunnel with the NHS. The output on NHC 2 is similar.

# Ping the private address 192.168.4.163 of NHC 2 from NHC 1.

```

[NHC1] ping 192.168.4.163
Ping 192.168.4.163 (192.168.4.163): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.4.163: icmp_seq=0 ttl=255 time=3.314 ms
56 bytes from 192.168.4.163: icmp_seq=1 ttl=255 time=2.786 ms
56 bytes from 192.168.4.163: icmp_seq=2 ttl=255 time=2.317 ms
56 bytes from 192.168.4.163: icmp_seq=3 ttl=255 time=3.060 ms
56 bytes from 192.168.4.163: icmp_seq=4 ttl=255 time=2.258 ms

```

```

--- Ping statistics for 192.168.4.163 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.258/2.747/3.314/0.411 ms

```

# Display detailed information about the NHRP table on NHC 1.

```
[NHC1] display nhrp map verbose
```

```

Interface : Tunnel0
 Destination/mask : 192.168.4.161/24
 Next hop : 192.168.4.161
 Creation time : 01:10:25
 Expiration time : never expire
 Type : static
 Flags : up ipsec
 NBMA address : 80.1.1.161

```

```

Interface : Tunnel0
 Destination/mask : 192.168.4.163/32
 Next hop : 192.168.4.163
 Creation time : 00:00:24
 Expiration time : 00:01:36
 Type : cached
 Flags : used up ipsec
 NBMA address : 80.1.1.163

```

# Display brief information about the NHRP session on NHC 1.

```
[NHC1] display mgre session
```

```

Interface : Tunnel0
Number of sessions: 2

```

| Peer NBMA address | Peer protocol address | Type | State     | State duration |
|-------------------|-----------------------|------|-----------|----------------|
| 80.1.1.161        | 192.168.4.161         | C-S  | Succeeded | 00:10:28       |
| 80.1.1.163        | 192.168.4.163         | C-C  | Succeeded | 00:00:32       |

The output indicates that NHC 1 has established a permanent tunnel with the NHS and a temporary tunnel with NHC 2. Both tunnels are protected by IPsec. The output on NHC 2 is similar.

# Display IKE SA information on NHC 1. The output on NHC 2 is similar.

```
[NHC1] display ike sa
```

| Connection-ID | Remote     | Flag | DOI   |
|---------------|------------|------|-------|
| 240           | 80.1.1.161 | RD   | IPsec |
| 241           | 80.1.1.163 | RD   | IPsec |

Flags:

RD--READY RL--REPLACED FD-FADING

# Display IPsec SA information on NHC 1. The output on NHC 2 is similar.

```
[NHC1] display ipsec sa
```

```

Interface: Tunnel0

IPsec profile: abc

```

Mode: ISAKMP

-----

Tunnel id: 4

Encapsulation mode: transport

Perfect forward secrecy:

Path MTU: 1398

Tunnel:

local address: 80.1.1.162

remote address: 80.1.1.163

Flow:

sour addr: 80.1.1.162/255.255.255.255 port: 0 protocol: gre

dest addr: 80.1.1.163/255.255.255.255 port: 0 protocol: gre

[Inbound ESP SAs]

SPI: 1566691874 (0x5d61d222)

Connection ID: 21474836488

Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843200/3584

Max received sequence-number: 0

Anti-replay check enable: Y

Anti-replay window size: 64

UDP encapsulation used for NAT traversal: N

Status: Active

[Outbound ESP SAs]

SPI: 1199855674 (0x4784583a)

Connection ID: 12884901895

Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/3584

Max sent sequence-number: 4

UDP encapsulation used for NAT traversal: N

Status: Active

-----

IPsec profile: abc

Mode: ISAKMP

-----

Tunnel id: 5

Encapsulation mode: transport

Perfect forward secrecy:

Path MTU: 1398

Tunnel:

local address: 80.1.1.162

remote address: 80.1.1.161

Flow:

sour addr: 80.1.1.162/255.255.255.255 port: 0 protocol: gre

```
dest addr: 80.1.1.161/255.255.255.255 port: 0 protocol: gre
```

[Inbound ESP SAs]

```
SPI: 989656188 (0x3afcf47c)
Connection ID: 30064771081
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843198/3560
Max received sequence-number: 12
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

[Outbound ESP SAs]

```
SPI: 1408141582 (0x53ee890e)
Connection ID: 38654705674
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3560
Max sent sequence-number: 8
UDP encapsulation used for NAT traversal: N
Status: Active
```

## IPsec-protected NHS-NHC mGRE network configuration example

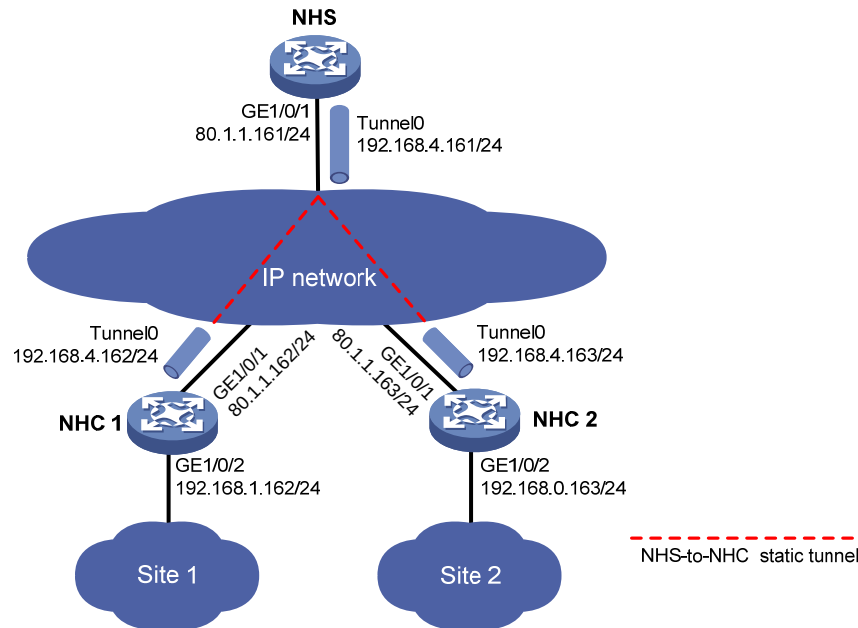
### Network requirements

As shown in [Figure 187](#), construct an NHS-NHC mGRE network. The NHS manages and maintains information for each node and forwards packets between NHCs.

Set up permanent (static) mGRE tunnels between the NHS and NHCs.

Configure IPsec to protect the mGRE tunnels.

**Figure 187 Network diagram**



## Configuration procedure

### 1. Configure NHC 1:

```
Configure an IP address for GigabitEthernet 1/0/1.
<NHC1> system-view
[NHC1] interface gigabitethernet 1/0/1
[NHC1-GigabitEthernet1/0/1] ip address 80.1.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC1] interface gigabitethernet 1/0/2
[NHC1-GigabitEthernet1/0/1] ip address 192.168.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/1] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] ip address 192.168.4.162 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC1-Tunnel0] ospf network p2mp
Enable OSPF for the tunnel interface.
[NHC1-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC1-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC1-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC1-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC1-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
```

```

[NHC1-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC1-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC1-Tunnel0] quit
Configure basic OSPF.
[NHC1] ospf 1
[NHC1-ospf-1] area 0.0.0.1
[NHC1-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[NHC1-ospf-1-area-0.0.0.1] quit
Configure an IPsec transform set named aa. Specify the encryption algorithm as 56-bit DES
and authentication algorithm as HMAC-SHA1.
[NHC1] ipsec transform-set aa
[NHC1-ipsec-transform-set-aa] esp encryption-algorithm des-cbc
[NHC1-ipsec-transform-set-aa] esp authentication-algorithm sha1
[NHC1-ipsec-transform-set-aa] quit
Create an IKE keychain named 1.
[NHC1] ike keychain 1
Configure the pre-shared key used with the peer 80.1.1.161 as a plaintext string of 12345678.
[NHC1-ike-keychain-1] pre-shared-key address 80.1.1.161 24 key simple 12345678
[NHC1-ike-keychain-1] quit
Create an IKE profile named abc.
[NHC1] ike profile abc
Specify IKE keychain 1 for the IKE profile.
[NHC1-ike-profile-abc] keychain 1
[NHC1-ike-profile-abc] quit
Create an IKE-based IPsec profile named abc.
[NHC1] ipsec profile abc isakmp
Specify IPsec transform set aa for the IPsec profile.
[NHC1-ipsec-profile-isakmp-abc] transform-set aa
Specify IKE profile abc for the IPsec profile.
[NHC1-ipsec-profile-isakmp-abc] ike-profile abc
[NHC1-ipsec-profile-isakmp-abc] quit
Apply IPsec profile abc to the mGRE tunnel interface.
[NHC2] interface tunnel0 mode mgre
[NHC1-Tunnel0] tunnel protection ipsec profile abc
[NHC1-Tunnel0] quit

```

## 2. Configure NHC 2:

```

Configure an IP address for GigabitEthernet 1/0/1.
<NHC2> system-view
[NHC2] interface gigabitethernet 1/0/1
[NHC2-GigabitEthernet1/0/1] ip address 80.1.1.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC2] interface gigabitethernet 1/0/2
[NHC2-GigabitEthernet1/0/1] ip address 192.168.0.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit

```



```

Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] ip address 192.168.4.163 255.255.255.0
Specify the OSPF interface network type as broadcast.
[NHC2-Tunnel0] ospf network p2mp
Enable OSPF for the tunnel interface.
[NHC2-Tunnel0] ospf 1 area 0.0.0.1
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC2-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC2-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC2-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC2-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 3600 seconds.
[NHC2-Tunnel0] nhrp holdtime 3600
Configure an NHS private-to-public address mapping.
[NHC2-Tunnel0] nhrp nhs 192.168.4.161 nbma 80.1.1.161
[NHC2-Tunnel0] quit
Configure basic OSPF.
[NHC2] ospf 1
[NHC2-ospf-1] area 0.0.0.1
[NHC2-ospf-1-area-0.0.0.1] network 192.168.4.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] network 192.168.0.0 0.0.0.255
[NHC2-ospf-1-area-0.0.0.1] quit
Configure an IPsec transform set named aa. Specify the encryption algorithm as 56-bit DES
and authentication algorithm as HMAC-SHA1.
[NHC2] ipsec transform-set aa
[NHC2-ipsec-transform-set-aa] esp encryption-algorithm des-cbc
[NHC2-ipsec-transform-set-aa] esp authentication-algorithm sha1
[NHC2-ipsec-transform-set-aa] quit
Create an IKE keychain named 1.
[NHC2] ike keychain 1
Configure the pre-shared key used with the peer 80.1.1.161 as a plaintext string of 12345678.
[NHC2-ike-keychain-1] pre-shared-key address 80.1.1.161 24 key simple 12345678
[NHC2-ike-keychain-1] quit
Create an IKE profile named abc.
[NHC2] ike profile abc
Specify IKE keychain 1 for the IKE profile.
[NHC2-ike-profile-abc] keychain 1
[NHC2-ike-profile-abc] quit
Create an IKE-based IPsec profile named abc.
[NHC2] ipsec profile abc isakmp
Specify IPsec transform set aa for the IPsec profile.
[NHC2-ipsec-profile-isakmp-abc] transform-set aa
Specify IKE profile abc for the IPsec profile.

```

```

[NHC2-ipsec-profile-isakmp-abc] ike-profile abc
[NHC2-ipsec-profile-isakmp-abc] quit
Apply IPsec profile abc to the mGRE tunnel interface.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] tunnel protection ipsec profile abc
[NHC2-Tunnel0] quit

```

## Verifying the configuration

# Display detailed information about the NHRP table on NHC 1.

```

[NHC1] display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 08:17:14
Expiration time : never expire
Type : static
Flags : up ipsec
NBMA address : 80.1.1.161

```

# Display brief information about the NHRP session on NHC 1.

```

[NHC1] display mgre session
Interface : Tunnel0
Number of sessions: 1

```

| Peer NBMA address | Peer protocol address | Type | State     | State duration |
|-------------------|-----------------------|------|-----------|----------------|
| 80.1.1.161        | 192.168.4.161         | C-S  | Succeeded | 00:00:18       |

The output indicates that NHC 1 has established a permanent tunnel with the NHS. The output on NHC 2 is similar.

# On NHC 1, test the connectivity between Site 1 and Site 2. The ping operation succeeds.

```

[NHC1] ping -a 192.168.1.162 192.168.0.163
Ping 192.168.0.163 (192.168.0.163) from 192.168.1.162: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.163: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 192.168.0.163: icmp_seq=1 ttl=254 time=17.000 ms
56 bytes from 192.168.0.163: icmp_seq=2 ttl=254 time=14.000 ms
56 bytes from 192.168.0.163: icmp_seq=3 ttl=254 time=7.000 ms
56 bytes from 192.168.0.163: icmp_seq=4 ttl=254 time=7.000 ms

--- Ping statistics for 192.168.0.163 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 7.000/11.000/17.000/3.950 ms

```

# Display IKE SA information on NHC 1. The output on NHC 2 is similar.

```

[NHC1] display ike sa

```

| Connection-ID | Remote     | Flag | DOI   |
|---------------|------------|------|-------|
| 3             | 80.1.1.161 | RD   | IPsec |

```

Flags:
RD--READY RL--REPLACED FD-FADING

```

# Display IPsec SA information on NHC 1. The output on NHC 2 is similar.

```

[NHC1] display ipsec sa

```

```

Interface: Tunnel0

IPsec profile: abc
Mode: ISAKMP

Tunnel id: 5
Encapsulation mode: transport
Perfect forward secrecy:
Path MTU: 1398
Tunnel:
 local address: 80.1.1.162
 remote address: 80.1.1.161
Flow:
 sour addr: 80.1.1.162/255.255.255.255 port: 0 protocol: gre
 dest addr: 80.1.1.161/255.255.255.255 port: 0 protocol: gre

[Inbound ESP SAs]
SPI: 2791687835 (0xa665c69b)
Connection ID: 12884901898
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3520
Max received sequence-number: 9
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 1369008262 (0x51996886)
Connection ID: 12884901897
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3520
Max sent sequence-number: 10
UDP encapsulation used for NAT traversal: N
Status: Active

```

## Full-mesh mGRE network with NAT traversal configuration example

### Network requirements

As shown in [Figure 188](#), the NHS and NHCs reside behind NAT gateways. Construct a full-mesh mGRE network. The NHS manages and maintains information for each node.

Set up permanent (static) mGRE tunnels between the NHS and NHCs. Set up temporary (dynamic) mGRE tunnels between NHCs when they need to communicate with each other.

**Figure 188 Network diagram**

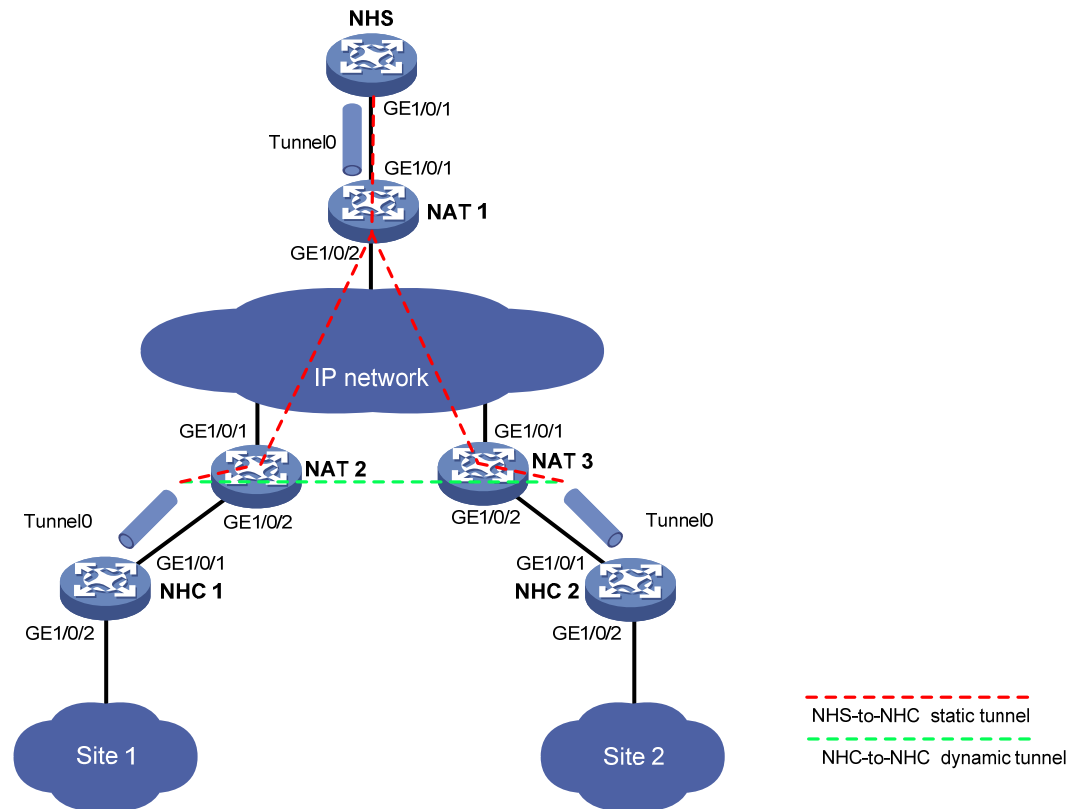


**Table 16 Interface and IP address assignment**

| Device | Interface | IP address       | Device | Interface | IP address  |
|--------|-----------|------------------|--------|-----------|-------------|
| NHC 1  | GE1/0/1   | 80.1.2.162/24    | NAT 1  | GE1/0/1   | 80.1.1.4/24 |
|        | GE1/0/2   | 192.168.1.162/24 |        | GE1/0/2   | 40.1.1.4/24 |
|        | Tunnel0   | 192.168.4.162/24 | NAT 2  | GE1/0/1   | 40.1.1.2/24 |
| NHC 2  | GE1/0/1   | 80.1.3.163/24    |        | GE1/0/2   | 80.1.2.2/24 |
|        | GE1/0/2   | 192.168.0.163/24 | NAT 3  | GE1/0/1   | 40.1.1.3/24 |
|        | Tunnel0   | 192.168.4.163/24 |        | GE1/0/2   | 80.1.3.3/24 |

## Configuration procedure

### ⚠ CAUTION:

The aging time for sessions in RAWIP-OPEN state set on NAT devices must be greater than the hold time for NHRP mapping entries set on NHCs. For information about setting the aging time and holdtime, see the **session aging-time state** command and the **nhrp holdtime** command, respectively.

1. Configure NHC 1:  
# Configure an IP address for GigabitEthernet 1/0/1.  
<NHC1> system-view  
[NHC1] interface gigabitethernet 1/0/1

```

[NHC1-GigabitEthernet1/0/1] ip address 80.1.2.162 255.255.255.0
[NHC1-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC1] interface gigabitethernet 1/0/2
[NHC1-GigabitEthernet1/0/2] ip address 192.168.1.162 255.255.255.0
[NHC1-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC1] interface tunnel0 mode mgre
[NHC1-Tunnel0] ip address 192.168.4.162 255.255.255.0
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC1-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC1-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC1-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC1-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 240 seconds.
[NHC1-Tunnel0] nhrp holdtime 240
Configure an NHS private-to-public address mapping.
[NHC1-Tunnel0] nhrp nhs 192.168.4.161 nbma 40.1.1.9
[NHC1-Tunnel0] quit
Configure static routes.
[NHC1] ip route-static 40.1.1.0 24 80.1.2.2
[NHC1] ip route-static 192.168.0.0 24 192.168.4.163

```

## 2. Configure NHC 2:

```

Configure an IP address for GigabitEthernet 1/0/1.
<NHC2> system-view
[NHC2] interface gigabitethernet 1/0/1
[NHC2-GigabitEthernet1/0/1] ip address 80.1.1.163 255.255.255.0
[NHC2-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NHC2] interface gigabitethernet 1/0/2
[NHC2-GigabitEthernet1/0/2] ip address 192.168.0.163 255.255.255.0
[NHC2-GigabitEthernet1/0/2] quit
Configure an IP address for mGRE tunnel interface Tunnel0.
[NHC2] interface tunnel0 mode mgre
[NHC2-Tunnel0] ip address 192.168.4.163 255.255.255.0
Specify GigabitEthernet 1/0/1 as the source interface of the mGRE tunnel.
[NHC2-Tunnel0] source gigabitethernet 1/0/1
Set the GRE key to 100000.
[NHC2-Tunnel0] gre key 100000
Set the NHRP network ID to 9.
[NHC2-Tunnel0] nhrp network-id 9
Configure the NHRP packet authentication key as a plaintext string of 123456.
[NHC2-Tunnel0] nhrp authentication simple 12345678
Set the holdtime of NHRP mapping entries to 240 seconds.

```

```

[NHC2-Tunnel0] nhrp holdtime 240
Configure an NHS private-to-public address mapping.
[NHC2-Tunnel0] nhrp nhs 192.168.4.161 nbma 40.1.1.9
[NHC2-Tunnel0] quit
Configure static routes.
[NHC2] ip route-static 40.1.1.0 24 80.1.3.3
[NHC2] ip route-static 192.168.1.0 24 192.168.4.162

```

**3. Configure NAT 1:**

```

Configure an IP address for GigabitEthernet 1/0/1.
<NAT1> system-view
[NAT1] interface gigabitethernet 1/0/1
[NAT1-GigabitEthernet1/0/1] ip address 80.1.1.4 255.255.255.0
[NAT1-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NAT1] interface gigabitethernet1/0/2
[NAT1-GigabitEthernet1/0/2] ip address 40.1.1.4 255.255.255.0
[NAT1-GigabitEthernet1/0/2] quit
Enable static NAT on GigabitEthernet 1/0/1.
[NAT1] interface gigabitethernet 1/0/1
[NAT1-GigabitEthernet1/0/1] nat static enable
[NAT1-GigabitEthernet1/0/1] quit
Configure an outbound static NAT mapping between interval IP address 80.1.1.161 and
external IP address 40.1.1.9.
[NAT1] nat static outbound 80.1.1.161 40.1.1.9

```

**4. Configure NAT 2:**

```

Configure an IP address for GigabitEthernet 1/0/1.
<NAT2> system-view
[NAT2] interface gigabitethernet 1/0/1
[NAT2-GigabitEthernet1/0/1] ip address 40.1.1.2 255.255.255.0
[NAT2-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NAT2] interface gigabitethernet 1/0/2
[NAT2-GigabitEthernet1/0/2] ip address 80.1.2.2 255.255.255.0
[NAT2-GigabitEthernet1/0/2] quit
Create NAT address group 0, and add addresses 40.1.1.5 and 40.1.1.6 to the group.
[NAT2] nat address-group 0
[NAT2-nat-address-group-0] address 40.1.1.5 40.1.1.6
[NAT2-nat-address-group-0] quit
Configure an outbound NO-PAT rule on interface GigabitEthernet 1/0/1 to translate the
source addresses of outgoing packets into the addresses in address group 0. Enable reverse
address translation.
[NAT2] interface gigabitethernet 1/0/1
[NAT2-GigabitEthernet1/0/1] nat outbound address-group 0 no-pat reversible
[NAT2-GigabitEthernet1/0/1] quit

```

**5. Configure NAT 3:**

```

Configure an IP address for GigabitEthernet 1/0/1.
<NAT3> system-view

```

```

[NAT3] interface gigabitethernet 1/0/1
[NAT3-GigabitEthernet1/0/1] ip address 40.1.1.3 255.255.255.0
[NAT3-GigabitEthernet1/0/1] quit
Configure an IP address for GigabitEthernet 1/0/2.
[NAT3] interface gigabitethernet 1/0/2
[NAT3-GigabitEthernet1/0/2] ip address 80.1.3.3 255.255.255.0
[NAT3-GigabitEthernet1/0/2] quit
Create NAT address group 0, and add addresses 40.1.1.7 and 40.1.1.8 to the group.
[NAT3] nat address-group 0
[NAT3-nat-address-group-0] address 40.1.1.7 40.1.1.8
[NAT3-nat-address-group-0] quit
Configure an outbound NO-PAT rule on interface GigabitEthernet 1/0/1 to translate the
source addresses of outgoing packets into the addresses in address group 0. Enable reverse
address translation.
[NAT3] interface gigabitethernet 1/0/1
[NAT3-GigabitEthernet1/0/1] nat outbound address-group 0 no-pat reversible
[NAT3-GigabitEthernet1/0/1] quit

```

## Verifying the configuration

# Display detailed information about the NHRP table on NHC 1.

```

<NHC1> display nhrp map verbose
Interface : Tunnel0
Destination/mask : 192.168.4.161/24
Next hop : 192.168.4.161
Creation time : 01:12:50
Expiration time : never expire
Type : static
Flags : up
NBMA address : 40.1.1.9

```

# Display brief information about the NHRP session on NHC 1.

```

<NHC1> display mgre session
Interface : Tunnel0
Number of sessions: 1
Peer NBMA address Peer protocol address Type State State duration
40.1.1.9 192.168.4.161 C-S Succeeded 01:12:43

```

The output indicates that NHC 1 has established a permanent tunnel with the NHS. The output on NHC 2 is similar.

# Ping the private address 192.168.4.163 of NHC 2 from NHC 1.

```

[NHC1] ping 192.168.4.163
Ping 192.168.4.163 (192.168.4.163): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.4.163: icmp_seq=0 ttl=255 time=3.314 ms
56 bytes from 192.168.4.163: icmp_seq=1 ttl=255 time=2.786 ms
56 bytes from 192.168.4.163: icmp_seq=2 ttl=255 time=2.317 ms
56 bytes from 192.168.4.163: icmp_seq=3 ttl=255 time=3.060 ms
56 bytes from 192.168.4.163: icmp_seq=4 ttl=255 time=2.258 ms

```

```

--- Ping statistics for 192.168.4.163 ---
5 packets transmitted, 5 packets received, 0.0% packet loss

```

round-trip min/avg/max/std-dev = 2.258/2.747/3.314/0.411 ms

# Display detailed information about the NHRP table on NHC 1.

[NHC1] display nhrp map verbose

Interface : Tunnel0  
Destination/mask : 192.168.4.161/24  
Next hop : 192.168.4.161  
Creation time : 01:10:25  
Expiration time : never expire  
Type : static  
Flags : up  
NBMA address : 40.1.1.9

Interface : Tunnel0  
Destination/mask : 192.168.4.163/32  
Next hop : 192.168.4.163  
Creation time : 00:00:24  
Expiration time : 00:01:36  
Type : cached  
Flags : used up  
NBMA address : 40.1.1.8

# Display brief information about the NHRP session on NHC 1.

[NHC1] display mgre session

Interface : Tunnel0

Number of sessions: 2

| Peer NBMA address | Peer protocol address | Type | State     | State duration |
|-------------------|-----------------------|------|-----------|----------------|
| 40.1.1.9          | 192.168.4.161         | C-S  | Succeeded | 00:10:28       |
| 40.1.1.8          | 192.168.4.163         | C-C  | Succeeded | 00:00:32       |

The output indicates that NHC 1 has established a permanent tunnel with the NHS and a temporary tunnel with NHC 2. The output on NHC 2 is similar.



# Document conventions and icons

## Conventions

This section describes the conventions used in the documentation.

### Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

### Command conventions

| Convention        | Description                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Boldface</b>   | <b>Bold</b> text represents commands and keywords that you enter literally as shown.                                                                     |
| <i>Italic</i>     | <i>Italic</i> text represents arguments that you replace with actual values.                                                                             |
| [ ]               | Square brackets enclose syntax choices (keywords or arguments) that are optional.                                                                        |
| { x   y   ... }   | Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.                                                   |
| [ x   y   ... ]   | Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.                                  |
| { x   y   ... } * | Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.                          |
| [ x   y   ... ] * | Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none. |
| &<1-n>            | The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.                                              |
| #                 | A line that starts with a pound (#) sign is comments.                                                                                                    |

### GUI conventions

| Convention      | Description                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Boldface</b> | Window names, button names, field names, and menu items are in Boldface. For example, the <b>New User</b> window appears; click <b>OK</b> . |
| >               | Multi-level menus are separated by angle brackets. For example, <b>File &gt; Create &gt; Folder</b> .                                       |

### Symbols

| Convention                                                                                            | Description                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>WARNING!</b>   | An alert that calls attention to important information that if not understood or followed can result in personal injury.                                               |
|  <b>CAUTION:</b>   | An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software. |
|  <b>IMPORTANT:</b> | An alert that calls attention to essential information.                                                                                                                |
| <b>NOTE:</b>                                                                                          | An alert that contains additional or supplementary information.                                                                                                        |
|  <b>TIP:</b>       | An alert that provides helpful information.                                                                                                                            |

# Network topology icons

| Convention                                                                          | Description                                                                                                                                |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
|    | Represents a generic network device, such as a router, switch, or firewall.                                                                |
|    | Represents a routing-capable device, such as a router or Layer 3 switch.                                                                   |
|    | Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features. |
|    | Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.              |
|    | Represents an access point.                                                                                                                |
|    | Represents a wireless terminator unit.                                                                                                     |
|    | Represents a wireless terminator.                                                                                                          |
|   | Represents a mesh access point.                                                                                                            |
|  | Represents omnidirectional signals.                                                                                                        |
|  | Represents directional signals.                                                                                                            |
|  | Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.                           |
|  | Represents a security card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.                                      |

# Support and other resources

## Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:  
[www.hpe.com/assistance](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:  
[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

### Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

## Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:  
[www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
  - Software Depot website:  
[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:  
[www.hpe.com/support/AccessToSupportMaterials](http://www.hpe.com/support/AccessToSupportMaterials)

---

### ! IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

---

## Websites

| Website                                                       | Link                                                                                                       |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Networking websites</b>                                    |                                                                                                            |
| Hewlett Packard Enterprise Information Library for Networking | <a href="http://www.hpe.com/networking/resourcefinder">www.hpe.com/networking/resourcefinder</a>           |
| Hewlett Packard Enterprise Networking website                 | <a href="http://www.hpe.com/info/networking">www.hpe.com/info/networking</a>                               |
| Hewlett Packard Enterprise My Networking website              | <a href="http://www.hpe.com/networking/support">www.hpe.com/networking/support</a>                         |
| Hewlett Packard Enterprise My Networking Portal               | <a href="http://www.hpe.com/networking/mynetworking">www.hpe.com/networking/mynetworking</a>               |
| Hewlett Packard Enterprise Networking Warranty                | <a href="http://www.hpe.com/networking/warranty">www.hpe.com/networking/warranty</a>                       |
| <b>General websites</b>                                       |                                                                                                            |
| Hewlett Packard Enterprise Information Library                | <a href="http://www.hpe.com/info/enterprise/docs">www.hpe.com/info/enterprise/docs</a>                     |
| Hewlett Packard Enterprise Support Center                     | <a href="http://www.hpe.com/support/hpesc">www.hpe.com/support/hpesc</a>                                   |
| Hewlett Packard Enterprise Support Services Central           | <a href="http://ssc.hpe.com/portal/site/ssc/">ssc.hpe.com/portal/site/ssc/</a>                             |
| Contact Hewlett Packard Enterprise Worldwide                  | <a href="http://www.hpe.com/assistance">www.hpe.com/assistance</a>                                         |
| Subscription Service/Support Alerts                           | <a href="http://www.hpe.com/support/e-updates">www.hpe.com/support/e-updates</a>                           |
| Software Depot                                                | <a href="http://www.hpe.com/support/softwaredepot">www.hpe.com/support/softwaredepot</a>                   |
| Customer Self Repair (not applicable to all devices)          | <a href="http://www.hpe.com/support/selfrepair">www.hpe.com/support/selfrepair</a>                         |
| Insight Remote Support (not applicable to all devices)        | <a href="http://www.hpe.com/info/insightremotesupport/docs">www.hpe.com/info/insightremotesupport/docs</a> |

## Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

[www.hpe.com/support/selfrepair](http://www.hpe.com/support/selfrepair)

## Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

[www.hpe.com/info/insightremotesupport/docs](http://www.hpe.com/info/insightremotesupport/docs)

## Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hpe.com](mailto:docsfeedback@hpe.com)). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

# Index

## Numerics

### 3DES

- IPsec encryption algorithm, [288](#)

### 802.1X

- access control method, [97](#)

- ACL assignment, [92](#)

- ACL assignment configuration, [111](#)

- architecture, [79](#)

- authentication, [83](#)

- authentication (access device initiated), [82](#)

- authentication (client initiated), [82](#)

- authentication configuration, [106](#)

- authentication initiation, [82](#)

- authentication request attempts max, [98](#)

- authentication timeout timers, [98](#)

- authentication trigger, [100](#)

- Auth-Fail VLAN, [91](#)

- Auth-Fail VLAN configuration, [102](#)

- authorization VLAN, [88](#)

- authorization VLAN assignment configuration, [108](#)

- basic configuration, [106](#)

- configuration, [88](#), [95](#)

- controlled/uncontrolled port, [79](#)

- critical VLAN, [91](#)

- critical VLAN configuration, [103](#)

- display, [106](#)

- EAD assistant configuration, [104](#)

- EAD assistant configuration (DHCP relay agent), [112](#)

- EAD assistant configuration (DHCP server), [115](#)

- EAD assistant feature, [93](#)

- EAP over RADIUS, [81](#)

- EAP packet format, [80](#)

- EAP relay authentication, [84](#)

- EAP relay enable, [96](#)

- EAP relay termination, [86](#)

- EAP relay/termination authentication, [84](#)

- EAP termination enable, [96](#)

- EAP-Message attribute, [81](#)

- EAPOL packet format, [81](#)

- enable, [95](#)

- feature cooperation, [92](#)

- guest VLAN, [90](#)

- guest VLAN assignment configuration, [108](#)

- guest VLAN configuration, [102](#)

- MAC authentication delay, [125](#)

- MAC-based access control, [88](#)

- maintain, [106](#)

- mandatory port authentication domain, [100](#)

- online user handshake, [99](#)

- overview, [79](#)

- packet format, [80](#)

- periodic online user reauthentication, [101](#)

- port authorization state, [96](#)

- port authorization status, [79](#)

- port security authentication control mode, [202](#)

- port security client

  - macAddressElseUserLoginSecure, [218](#)

  - port security client userLoginWithOUI, [215](#)

- port security configuration, [202](#), [205](#), [213](#)

- port security features, [208](#)

- port security intrusion protection, [208](#)

- port security MAC address autoLearn, [213](#)

- port security MAC move, [211](#)

- port security MAC+802.1X authentication, [204](#)

- port security mode, [206](#)

- port security NTK, [208](#)

- port users max, [98](#)

- port-based access control, [88](#)

- quiet timer, [101](#)

- RADIUS Message-Authentication attribute, [82](#)
- related protocols, [80](#)
- SmartOn configuration, [105](#)
- SmartOn feature, [93](#)
- SmartOn feature configuration, [117](#)
- supported domain name delimiters, [103](#)
- troubleshooting, [119](#)
- user profile configuration, [223](#)
- VLAN manipulation, [88](#)

## A

### AAA

- concurrent login user max, [56](#)
- configuration, [1](#), [18](#), [58](#)
- device implementation, [12](#)
- display, [58](#)
- displaying local users/user groups, [24](#)
- FIPS compliance, [18](#)
- HWTACACS accounting server, [37](#)
- HWTACACS authentication server, [36](#)
- HWTACACS authorization server, [37](#)
- HWTACACS display, [41](#)
- HWTACACS implementation, [7](#)
- HWTACACS maintain, [41](#)
- HWTACACS outgoing packet source IP address, [39](#)
- HWTACACS scheme, [36](#)
- HWTACACS scheme creation, [36](#)
- HWTACACS scheme VPN, [38](#)
- HWTACACS server PPP user, [75](#)
- HWTACACS server SSH user, [63](#)
- HWTACACS shared keys, [38](#)
- HWTACACS timers, [40](#)
- HWTACACS traffic statistics units, [39](#)
- HWTACACS username format, [39](#)
- HWTACACS/RADIUS differences, [7](#)
- IPsec IKEv2 address pool, [372](#)
- ISP domain accounting method, [52](#)
- ISP domain attribute configuration, [47](#)

- ISP domain authentication method, [49](#)
- ISP domain authorization method, [51](#)
- ISP domain creation, [46](#)
- ISP domain method, [46](#)
- ITA policy configuration, [56](#)
- LDAP administrator attribute, [43](#)
- LDAP attribute map, [44](#)
- LDAP attribute map for authorization, [45](#)
- LDAP authentication server, [45](#)
- LDAP authorization server, [45](#)
- LDAP display, [46](#)
- LDAP implementation, [9](#)
- LDAP scheme, [42](#)
- LDAP scheme creation, [45](#)
- LDAP server creation, [42](#)
- LDAP server IP address, [42](#)
- LDAP server SSH user authentication, [65](#)
- LDAP server SSL VPN user authentication+authorization, [70](#)
- LDAP user attribute, [43](#)
- LDAP versions, [42](#)
- local SSH user authentication+authorization, [62](#)
- local user attribute, [21](#)
- local user configuration, [20](#)
- methods, [13](#)
- MPLS L3VPN implementation, [14](#)
- NAS-ID profile configuration, [57](#)
- protocols and standards, [14](#)
- RADIUS accounting server parameters, [27](#)
- RADIUS accounting-on enable, [32](#)
- RADIUS accounting-on enable (extended), [33](#)
- RADIUS Acct-Session-Id format, [57](#)
- RADIUS attributes, [15](#)
- RADIUS authentication server, [26](#)
- RADIUS DAE server, [55](#)
- RADIUS display, [35](#)
- RADIUS implementation, [2](#)
- RADIUS maintain, [35](#)
- RADIUS packet DSCP priority, [55](#)

- RADIUS request transmission attempts
  - max, [29](#)
- RADIUS scheme, [25](#)
- RADIUS scheme creation, [26](#)
- RADIUS scheme VPN, [28](#)
- RADIUS security policy server IP address, [33](#)
- RADIUS server SSH user
  - authentication+authorization, [58](#)
- RADIUS server status, [29](#)
- RADIUS session-control, [54](#)
- RADIUS shared keys, [28](#)
- RADIUS SNMP notification, [35](#)
- RADIUS timers, [31](#)
- RADIUS traffic statistics units, [28](#)
- RADIUS username format, [28](#)
- scheme configuration, [19](#)
- troubleshoot HWTACACS, [78](#)
- troubleshoot LDAP user authentication
  - fails, [78](#)
- troubleshoot RADIUS, [76](#)
- troubleshoot RADIUS accounting error, [77](#)
- troubleshoot RADIUS authentication
  - failure, [76](#)
- troubleshoot RADIUS packet delivery
  - failure, [77](#)
- user group attribute, [23](#)
- user management by ISP domains, [12](#)
- user management by user access types, [12](#)

accelerating

- object policy rule matching acceleration, [498](#)

access control

- security portal authentication, [139](#)
- security portal authentication
  - configuration, [134](#), [157](#)

access control policy

- PKI certificate-based access control
  - policy, [274](#)

accessing

- security portal authentication device access, [135](#)

account idle time (password control), [227](#)

accounting

- AAA configuration, [1](#), [18](#), [58](#)
- AAA ISP domain accounting method, [52](#)
- AAA ITA policy configuration, [56](#)
- AAA RADIUS accounting-on, [32](#)
- AAA RADIUS accounting-on (extended), [33](#)
- AAA RADIUS Acct-Session-Id format, [57](#)
- session management statistics collection, [482](#)

ACK flood, [514](#)

ACL

- 802.1X ACL assignment, [92](#)
- 802.1X+ACL assignment configuration, [111](#)
- APR PBAR host port mapping (ACL-based), [474](#)
- attack D&P detection exemption, [518](#)
- IPsec ACL, [292](#)
- IPsec ACL de-encapsulated packet check, [304](#)
- IPsec ACL rule keywords, [292](#)
- IPsec ACL-based implementation, [289](#), [292](#)
- IPsec ACL-based tunnel establishment, [291](#)
- IPsec mirror image ACLs, [294](#)
- IPsec non-mirror image ACLs, [294](#)
- IPv6 uRPF default route, [571](#)
- MAC authentication ACL assignment, [121](#), [131](#)
- SSH management parameters, [400](#)
- uRPF, [564](#)

active

- ARP active acknowledgement, [551](#)
- security portal authentication type, [134](#)

address

- IPv6 uRPF configuration, [571](#), [574](#), [575](#)
- uRPF configuration, [564](#), [568](#), [569](#)

address pool

- IPsec IKEv2 address pool, [372](#)

Address Resolution Protocol. Use [ARP](#)

Advanced Stateful Packet Filter. See [ASPF](#)

AES

- IPsec encryption algorithm, [288](#)



- aging
  - session management aging time (application layer protocol), [481](#)
  - session management aging time (protocol state), [480](#)
- AH
  - IPsec security protocol [51](#), [286](#)
- alert protocol (SSL), [455](#)
- algorithm
  - IPsec authentication, [288](#)
  - IPsec encryption (3DES), [288](#)
  - IPsec encryption (AES), [288](#)
  - IPsec encryption (DES), [288](#)
  - IPsec IKE DH algorithm, [333](#)
  - SSH negotiation, [393](#)
- anti-replay
  - IPsec anti-replay redundancy, [305](#)
  - IPsec configuration, [305](#)
- any authentication (SSH), [393](#)
- application
  - IPsec application-based implementation, [290](#)
  - IPsec application-based tunnel establishment, [291](#)
  - IPv6 uRPF network, [574](#)
  - uRPF network, [568](#)
- application recognition. See [APR](#)
- applying
  - AAA ITA policy, [56](#)
  - ASPF policy (interface), [466](#)
  - ASPF policy (zone pair), [466](#)
  - attack D&P policy application (device), [519](#)
  - attack D&P policy application (interface), [519](#)
  - connection limit policy, [488](#)
  - interface NAS ID profile, [156](#)
  - IPsec policy to interface, [303](#)
  - IPsec profile to tunnel interface (IKE-based), [312](#)
  - IPv4 object policy to zone pair, [498](#)
  - IPv6 object policy to zone pair, [498](#)
  - port security NAS-ID profile, [212](#)
- APR
  - application group configuration, [476](#)
  - application statistics enable, [476](#)
  - configuration, [474](#), [478](#)
  - display, [477](#)
  - group-based (predefined), [474](#)
  - group-based (user-defined), [474](#)
  - maintain, [477](#)
  - PBAR configuration, [475](#)
  - PBAR mapping, [474](#)
- architecture
  - 802.1X, [79](#)
  - PKI, [246](#)
- ARP
  - attack protection. See [ARP attack protection](#)
  - scanning configuration restrictions, [560](#)
- ARP attack protection
  - active acknowledgement, [551](#)
  - ARP detection display, [557](#)
  - ARP detection maintain, [557](#)
  - authorized ARP configuration, [551](#)
  - authorized ARP configuration (DHCP relay agent), [553](#)
  - authorized ARP configuration (DHCP server), [552](#)
  - command and hardware compatibility, [546](#)
  - configuration, [546](#)
  - detection configuration, [554](#)
  - filtering configuration, [562](#), [563](#)
  - fixed ARP configuration, [560](#)
  - gateway protection, [561](#), [561](#)
  - packet source MAC consistency check, [551](#)
  - packet validity check configuration, [556](#)
  - restricted forwarding, [556](#)
  - restricted forwarding configuration, [558](#)
  - scanning configuration, [560](#)
  - source MAC-based attack detection, [549](#), [550](#)
  - source MAC-based detection display, [549](#)
  - unresolvable IP attack, [547](#), [548](#)

- unresolvable IP attack blackhole routing, [547](#)
- unresolvable IP attack protection display, [547](#)
- unresolvable IP attack source suppression, [547](#)
- user validity check, [555](#)
- user+packet validity check, [557](#)

## ASPF

- application inspection (FTP), [467](#)
- application inspection (H.323), [470](#)
- application inspection (TCP), [468](#)
- application layer protocol inspection, [463](#)
- APR configuration, [474](#)
- basic concepts, [462](#)
- configuration, [462](#), [465](#), [467](#)
- display, [467](#)
- inspection, [463](#)
- maintain, [467](#)
- policy application (interface), [466](#)
- policy application (zone pair), [466](#), [471](#)
- policy configuration, [465](#)
- session management, [479](#)
- session management configuration, [480](#)
- transport layer protocol inspection, [464](#)

## assigning

- 802.1X ACL assignment, [92](#)
- MAC authentication ACL, [131](#)

## associating

- IPsec SA, [288](#)

## attack

- ARP attack protection configuration, [546](#)

## attack D&P

- blacklist, [506](#)
- blacklist configuration, [522](#), [531](#)
- client verification, [507](#)
- client verification (DNS), [509](#), [521](#)
- client verification (HTTP), [510](#), [522](#)
- client verification (TCP), [507](#), [520](#)
- client verification configuration (DNS), [533](#)
- client verification configuration (HTTP), [534](#)

- client verification configuration (TCP), [532](#)
- command and hardware compatibility, [503](#)
- configuration, [503](#), [511](#), [528](#)
- configuration (interface-based), [528](#)
- defense policy configuration, [511](#)
- defense policy configuration (ACK flood), [514](#)
- defense policy configuration (DNS flood), [517](#)
- defense policy configuration (FIN flood), [515](#)
- defense policy configuration (flood), [513](#)
- defense policy configuration (HTTP flood), [518](#)
- defense policy configuration (ICMP flood), [516](#)
- defense policy configuration (ICMPv6 flood), [516](#)
- defense policy configuration (RST flood), [515](#)
- defense policy configuration (scanning), [513](#)
- defense policy configuration (single-packet), [511](#)
- defense policy configuration (SYN flood), [514](#)
- defense policy configuration (SYN-ACK flood), [514](#)
- defense policy configuration (UDP flood), [517](#)
- defense policy creation, [511](#)
- detection exemption configuration, [518](#)
- device-preventable attacks, [503](#)
- display, [523](#)
- log aggregation disable, [520](#)
- maintain, [523](#)
- policy application (device), [519](#)
- policy application (interface), [519](#)
- TCP fragment attack prevention configuration, [520](#)

attack detection and prevention. See [attack D&P](#)

## attack prevention

- ASPF application inspection (FTP), [467](#)
- ASPF application inspection (H.323), [470](#)
- ASPF application inspection (TCP), [468](#)
- ASPF configuration, [462](#), [465](#), [467](#)

## attacking

- detection and prevention. See [attack D&P](#)

## attribute

- 802.1X RADIUS EAP-Message, [81](#)

- 802.1X RADIUS Message-Authentication, [82](#)
- AAA HWTACACS scheme, [36](#)
- AAA ISP domain attribute, [47](#)
- AAA LDAP administrator attribute, [43](#)
- AAA LDAP attribute map, [44](#)
- AAA LDAP attribute map for authorization, [45](#)
- AAA LDAP scheme, [42](#)
- AAA LDAP user attribute, [43](#)
- AAA local user, [20](#)
- AAA local user attribute, [21](#)
- AAA RADIUS, [15](#)
- AAA RADIUS common standard attributes, [15](#)
- AAA RADIUS extended attributes, [6](#)
- AAA RADIUS Hewlett Packard Enterprise proprietary attributes, [16](#)
- AAA RADIUS Login-Service attribute check method, [34](#)
- AAA RADIUS Remanent\_Volume attribute data measurement unit, [34](#)
- AAA RADIUS scheme, [25](#)
- AAA scheme, [19](#)
- AAA user group attribute, [23](#)
- authenticating
  - 802.1X access device initiated authentication, [82](#)
  - 802.1X authentication, [83](#)
  - 802.1X authentication request attempts max, [98](#)
  - 802.1X authentication trigger, [100](#)
  - 802.1X client-initiated, [82](#)
  - 802.1X EAP over RADIUS, [81](#)
  - 802.1X EAP relay authentication, [84](#)
  - 802.1X EAP relay enable, [96](#)
  - 802.1X EAP relay/termination, [84](#)
  - 802.1X EAP termination, [86](#)
  - 802.1X EAP termination enable, [96](#)
  - 802.1X initiation, [82](#)
  - 802.1X mandatory port authentication domain, [100](#)
  - 802.1X overview, [79](#)
  - 802.1X periodic online user reauthentication, [101](#)
  - 802.1X RADIUS Message-Authentication attribute, [82](#)
  - 802.1X SmartOn feature configuration, [117](#)
  - 802.1X timeout timers, [98](#)
  - 802.1X VLAN manipulation, [88](#)
  - AAA configuration, [1](#), [18](#), [58](#)
  - AAA ISP domain authentication method, [49](#)
  - AAA LDAP authentication, [9](#)
  - AAA local SSH user authentication+authorization, [62](#)
  - AAA RADIUS server SSH user authentication+authorization, [58](#)
  - AAA RADIUS user authentication methods, [2](#)
  - IPsec, [288](#)
  - IPsec authentication algorithms, [288](#)
  - IPsec Authentication Header. Use [AH](#)
  - IPsec configuration, [286](#), [314](#)
  - IPsec Encapsulating Security Payload. Use [ESP](#)
  - IPsec IKE configuration (aggressive mode+RSA signature authentication), [346](#)
  - IPsec IKE configuration (main mode/pre-shared key authentication), [342](#)
  - IPsec IKE DSA signature authentication, [332](#)
  - IPsec IKE pre-shared key authentication, [332](#)
  - IPsec IKE RSA signature authentication, [332](#)
  - IPsec IKEv2 configuration (pre-shared key authentication), [373](#)
  - IPsec IKEv2 configuration (RSA signature authentication), [377](#)
  - IPsec RIPng configuration, [324](#)
  - IPsec RRI configuration, [308](#), [327](#)
  - IPsec tunnel for IPv4 packets (IKE-based), [317](#)
  - IPsec tunnel for IPv4 packets (manual), [314](#)
  - IPsec tunnel for IPv6 (IKE-based), [320](#)
  - MAC authentication, [120](#), [123](#), [127](#)
  - MAC authentication (local), [127](#)
  - MAC authentication (RADIUS-based), [129](#)

- MAC authentication VLAN assignment, [121](#)
- password control configuration, [225](#), [228](#), [232](#)
- periodic MAC reauthentication, [121](#)
- port security authentication modes, [202](#)
- port security client
  - macAddressElseUserLoginSecure, [218](#)
  - port security client userLoginWithOUI, [215](#)
- port security configuration, [202](#), [205](#), [213](#)
- port security MAC address autoLearn, [213](#)
- security portal authentication client, [135](#)
- security portal authentication server, [135](#)
- SSH configuration, [392](#)
- SSH methods, [393](#)
- SSH SCP file transfer+password authentication, [444](#)
- SSH Secure Telnet client password authentication, [425](#)
- SSH Secure Telnet client publickey authentication, [429](#)
- SSH Secure Telnet server password authentication, [417](#)
- SSH Secure Telnet server publickey authentication, [420](#)
- SSH server configuration, [395](#)
- SSH SFTP client publickey authentication, [437](#)
- SSH SFTP server password authentication, [435](#)
- SSL services, [455](#)
- user profile, [224](#)
- user profile configuration, [223](#)
- authentication
  - LDAP process, [10](#)
- Authentication, Authorization, and Accounting. Use [AAA](#)
- Auth-Fail VLAN
  - 802.1X authentication, [91](#)
  - 802.1X configuration, [102](#)
- authorization
  - IPsec IKEv2 address pool, [372](#)

- LDAP process, [11](#)
- authorization VLAN
  - 802.1X assignment, [89](#)
  - 802.1X assignment configuration, [108](#)
  - 802.1X supported, [88](#)
  - 802.1X unsupported, [89](#)
- authorized ARP
  - configuration, [551](#)
  - configuration (DHCP relay agent), [553](#)
  - configuration (DHCP server), [552](#)
- authorizing
  - 802.1X authorization VLAN, [88](#)
  - 802.1X port authorization state, [96](#)
  - 802.1X port authorization status, [79](#)
  - 802.1X port authorized-force state, [96](#)
  - 802.1X port auto state, [96](#)
  - 802.1X port unauthorized-force state, [96](#)
  - AAA configuration, [1](#), [18](#), [58](#)
  - AAA ISP domain authorization method, [51](#)
  - AAA LDAP authorization, [9](#)
  - AAA local SSH user authentication+authorization, [62](#)
  - AAA RADIUS server SSH user authentication+authorization, [58](#)
  - AAA RADIUS session-control, [54](#)
  - port security authorization-fail-offline feature, [212](#)
  - port security server authorization information, [211](#)
- auto
  - FIPS mode (automatic reboot), [580](#)
  - FIPS mode entry (automatic reboot), [584](#)
  - FIPS mode exit (automatic reboot), [582](#), [587](#)
  - PKI certificate request (automatic), [252](#)
  - port security MAC address autoLearn, [213](#)

## B

### BAS-IP

- security portal authentication BAS-IP, [153](#)

### BGP

- mGRE routing configuration, [593](#)

## binding

- IP source guard (IPSG) dynamic binding, [537](#)
- IP source guard (IPSG) static binding, [536](#)
- IPsec source interface to policy, [306](#)
- IPv4 source guard (IPv4SG) dynamic binding configuration, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv4 source guard (IPv4SG) static binding configuration, [538](#), [540](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- IPv6 source guard (IPv6SG) static binding configuration, [539](#), [543](#)

## blackhole routing

- ARP attack protection blackhole routing (unresolvable IP attack), [547](#)

## blacklisting

- attack D&P, [506](#)
- attack D&P configuration, [522](#), [531](#)

## C

### CA

- PKI architecture, [246](#)
- PKI CA policy, [246](#)
- PKI certificate, [245](#)
- PKI certificate export, [256](#)
- PKI certificate obtain, [253](#)
- PKI certificate removal, [257](#)
- PKI certificate request, [251](#)
- PKI certificate request (automatic), [252](#)
- PKI certificate request (manual), [252](#)
- PKI certificate request abort, [253](#)
- PKI certificate verification, [254](#)
- PKI CRL, [245](#)
- PKI domain configuration, [249](#)
- PKI entity configuration, [248](#)
- PKI Keon CA server certificate request (NAT-PT network), [268](#)
- PKI OpenCA server certificate request, [265](#)

PKI RSA Keon CA server certificate request, [259](#)

PKI storage path, [256](#)

PKI Windows 2003 CA server certificate request, [261](#)

PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)

troubleshooting PKI CA certificate import failure, [283](#)

troubleshooting PKI CA certificate obtain failure, [281](#)

### CAR

AAA RADIUS class attribute as CAR parameter, [33](#)

### certificate

authority. Use [CA](#)

PKI certificate verification (CRL checking), [254](#)

PKI certificate verification (w/o CRL checking), [255](#)

PKI certificate-based access control policy, [274](#)  
revocation list. Use [CRL](#)

change cipher spec protocol (SSL), [455](#)

### changing

AAA RADIUS packet DSCP priority, [55](#)

IPv4 object policy rule match order, [498](#)

IPv6 object policy rule match order, [498](#)

### CHAP/PAP authentication

direct/cross-subnet portal authentication process, [137](#)

re-DHCP portal authentication process, [138](#)

### checking

IPsec ACL de-encapsulated packet check, [304](#)

IPv6 uRPF loose check mode, [571](#)

IPv6 uRPF strict check mode, [571](#)

PKI certificate verification (CRL checking), [254](#)

PKI certificate verification (w/o CRL checking), [255](#)

uRPF loose check mode, [564](#)

uRPF strict check mode, [564](#)

class attribute (RADIUS), [33](#)

- classifying
  - IPsec QoS pre-classify enable, [307](#)
- clearing
  - IPsec packet DF bit clear, [307](#)
- client
  - 802.1X authentication, [83](#)
  - 802.1X authentication (access device initiated), [82](#)
  - 802.1X authentication (client-initiated), [82](#)
  - 802.1X authentication client timeout timer, [98](#)
  - 802.1X authentication configuration, [106](#)
  - 802.1X authentication initiation, [82](#)
  - 802.1X authorization VLAN assignment configuration, [108](#)
  - 802.1X basic configuration, [106](#)
  - 802.1X configuration, [88](#), [95](#)
  - 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
  - 802.1X EAD assistant configuration (DHCP server), [115](#)
  - 802.1X guest VLAN assignment configuration, [108](#)
  - 802.1X SmartOn feature configuration, [117](#)
  - 802.1X+ACL assignment configuration, [111](#)
  - attack D&P client verification, [507](#)
  - attack D&P client verification (DNS), [509](#)
  - attack D&P client verification (HTTP), [510](#)
  - attack D&P client verification (TCP), [507](#)
  - security portal authentication, [135](#)
  - security portal authentication system components, [134](#)
  - SSL client policy configuration, [458](#)
- command
  - AAA command accounting method, [13](#)
  - AAA command authorization method, [13](#)
  - attack D&P command and hardware compatibility, [503](#)
- command and hardware compatibility
  - ARP attack protection, [546](#)
  - IPv6 uRPF, [574](#)
  - portal, [139](#)
  - uRPF, [568](#)
  - user profile, [223](#)
- communication
  - peer public key entry, [240](#)
- comparing
  - 802.1X EAP relay/termination authentication, [84](#)
- compatibility
  - attack D&P command and hardware compatibility, [503](#)
  - portal command and hardware compatibility, [139](#)
  - user profile, [223](#)
- complexity checking (password control), [225](#)
- composition checking (password control), [225](#)
- conditional self-test, [583](#)
- configuring
  - 802.1X, [88](#), [95](#)
  - 802.1X authentication, [106](#)
  - 802.1X authentication trigger, [100](#)
  - 802.1X Auth-Fail VLAN, [91](#), [102](#)
  - 802.1X authorization VLAN assignment, [108](#)
  - 802.1X basics, [106](#)
  - 802.1X critical VLAN, [91](#), [103](#)
  - 802.1X EAD assistant, [104](#)
  - 802.1X EAD assistant (DHCP relay agent), [112](#)
  - 802.1X EAD assistant (DHCP server), [115](#)
  - 802.1X guest VLAN, [90](#), [102](#)
  - 802.1X guest VLAN assignment, [108](#)
  - 802.1X online user handshake, [99](#)
  - 802.1X SmartOn, [105](#), [117](#)
  - 802.1X+ACL assignment, [111](#)
  - AAA, [1](#), [18](#), [58](#)
  - AAA Acct-Session-Id format, [57](#)
  - AAA HWTACACS schemes, [36](#)
  - AAA HWTACACS server PPP user, [75](#)
  - AAA HWTACACS server SSH users, [63](#)
  - AAA ISP domain accounting method, [52](#)
  - AAA ISP domain attribute, [47](#)



- AAA ISP domain authentication method, [49](#)
- AAA ISP domain authorization method, [51](#)
- AAA ISP domain method, [46](#)
- AAA ITA policy, [56](#)
- AAA LDAP administrator attributes, [43](#)
- AAA LDAP attribute map, [44](#)
- AAA LDAP scheme, [42](#)
- AAA LDAP server IP address, [42](#)
- AAA LDAP server SSH user authentication, [65](#)
- AAA LDAP server SSL VPN user authentication+authorization, [70](#)
- AAA LDAP user attributes, [43](#)
- AAA local SSH user authentication+authorization, [62](#)
- AAA local user, [20](#)
- AAA local user attributes, [21](#)
- AAA RADIUS DAE server, [55](#)
- AAA RADIUS Login-Service attribute check method, [34](#)
- AAA RADIUS scheme, [25](#)
- AAA RADIUS security policy server IP address, [33](#)
- AAA RADIUS server SSH user authentication+authorization, [58](#)
- AAA RADIUS server status detection test profile, [25](#)
- AAA scheme, [19](#)
- AAA user group attributes, [23](#)
- APR, [474](#), [478](#)
- APR application groups, [476](#)
- APR PBAR, [475](#)
- ARP active acknowledgement, [551](#)
- ARP attack detection (source MAC-based), [549](#), [550](#)
- ARP attack protection, [546](#)
- ARP attack protection (unresolvable IP attack), [547](#), [548](#)
- ARP attack protection blackhole routing (unresolvable IP attack), [547](#)

- ARP attack protection source suppression (unresolvable IP attack), [547](#)
- ARP detection, [554](#)
- ARP detection packet validity check, [556](#)
- ARP detection restricted forwarding, [556](#), [558](#)
- ARP detection user validity check, [555](#)
- ARP detection user+packet validity check, [557](#)
- ARP filtering, [562](#), [563](#)
- ARP gateway protection, [561](#), [561](#)
- ARP packet source MAC consistency check, [551](#)
- ARP scanning, [560](#)
- ASPF, [462](#), [465](#), [467](#)
- ASPF application inspection (FTP), [467](#)
- ASPF application inspection (H.323), [470](#)
- ASPF application inspection (TCP), [468](#)
- ASPF policy, [465](#)
- ASPF policy application (zone pair), [471](#)
- attack D&P, [503](#), [511](#), [528](#)
- attack D&P (interface-based), [528](#)
- attack D&P blacklist, [522](#), [531](#)
- attack D&P client verification (DNS), [521](#), [533](#)
- attack D&P client verification (HTTP), [522](#), [534](#)
- attack D&P client verification (TCP), [520](#), [532](#)
- attack D&P defense policy, [511](#)
- attack D&P defense policy (ACK flood), [514](#)
- attack D&P defense policy (DNS flood), [517](#)
- attack D&P defense policy (FIN flood), [515](#)
- attack D&P defense policy (flood), [513](#)
- attack D&P defense policy (HTTP flood), [518](#)
- attack D&P defense policy (ICMP flood), [516](#)
- attack D&P defense policy (ICMPv6 flood), [516](#)
- attack D&P defense policy (RST flood), [515](#)
- attack D&P defense policy (scanning), [513](#)
- attack D&P defense policy (single-packet), [511](#)
- attack D&P defense policy (SYN flood), [514](#)
- attack D&P defense policy (SYN-ACK flood), [514](#)
- attack D&P defense policy (UDP flood), [517](#)
- attack D&P detection exemption, [518](#)
- attack D&P policy application (device), [519](#)

- attack D&P policy application (interface), [519](#)
- attack D&P TCP fragment attack prevention, [520](#)
- authorized ARP, [551](#)
- authorized ARP (DHCP relay agent), [553](#)
- authorized ARP (DHCP server), [552](#)
- connection limit, [486](#), [489](#)
- connection limit (interface-based), [486](#)
- connection limit policy, [487](#)
- crypto engine, [577](#)
- crypto engine (hardware), [577](#)
- FIPS, [579](#), [584](#)
- FIPS mode, [580](#)
- fixed ARP, [560](#)
- IP source guard (IPSG), [536](#), [537](#), [540](#)
- IPsec, [286](#), [314](#)
- IPsec ACL, [292](#)
- IPsec ACL anti-replay, [305](#)
- IPsec anti-replay redundancy, [305](#)
- IPsec for IPv6 routing protocols, [309](#)
- IPsec for mGRE tunnel, [593](#)
- IPsec IKE, [331](#), [333](#), [342](#)
- IPsec IKE (aggressive mode+NAT traversal), [353](#)
- IPsec IKE (aggressive mode+RSA signature authentication), [346](#)
- IPsec IKE (main mode/pre-shared key authentication), [342](#)
- IPsec IKE DPD, [340](#)
- IPsec IKE global identity information, [338](#)
- IPsec IKE keepalive function, [339](#)
- IPsec IKE keychain, [337](#)
- IPsec IKE NAT keepalive function, [339](#)
- IPsec IKE profile, [334](#)
- IPsec IKE proposal, [336](#)
- IPsec IKE SNMP notification, [341](#)
- IPsec IKEv2, [363](#), [364](#), [373](#)
- IPsec IKEv2 (NAT traversal), [385](#)

- IPsec IKEv2 (pre-shared key authentication), [373](#)
- IPsec IKEv2 (RSA signature authentication), [377](#)
- IPsec IKEv2 address pool, [372](#)
- IPsec IKEv2 DPD, [371](#)
- IPsec IKEv2 global parameters, [371](#)
- IPsec IKEv2 keychain, [370](#)
- IPsec IKEv2 NAT keepalive, [372](#)
- IPsec IKEv2 policy, [368](#)
- IPsec IKEv2 profile, [365](#)
- IPsec IKEv2 proposal, [369](#)
- IPsec IPv6 routing protocol profile (manual), [309](#)
- IPsec packet DF bit, [307](#)
- IPsec policy (IKE-based), [299](#)
- IPsec policy (IKE-based/direct), [300](#)
- IPsec policy (IKE-based/template), [301](#)
- IPsec policy (manual), [297](#)
- IPsec profile (IKE-based), [311](#)
- IPsec RIPng, [324](#)
- IPsec RRI, [308](#), [327](#)
- IPsec SNMP notification, [312](#)
- IPsec transform set, [295](#)
- IPsec tunnel, [311](#)
- IPsec tunnel for IPv4 packets (IKE-based), [317](#)
- IPsec tunnel for IPv4 packets (manual), [314](#)
- IPsec tunnel for IPv6 packets (IKE-based), [320](#)
- IPv4 address object group, [493](#)
- IPv4 object policy rule, [496](#)
- IPv4 source guard (IPv4SG), [537](#)
- IPv4 source guard (IPv4SG) dynamic binding, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay, [542](#)
- IPv4 source guard (IPv4SG) static binding, [538](#), [540](#)
- IPv6 address object group, [493](#)
- IPv6 object policy rule, [496](#)
- IPv6 source guard (IPv6SG), [538](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping, [544](#)



- IPv6 source guard (IPv6SG) static binding, [539](#), [543](#)
- IPv6 uRPF, [571](#), [574](#), [575](#)
- MAC authentication, [120](#), [123](#), [127](#)
- MAC authentication (local), [127](#)
- MAC authentication (RADIUS-based), [129](#)
- MAC authentication ACL assignment, [131](#)
- MAC authentication delay, [125](#)
- MAC authentication keep-online, [126](#)
- MAC authentication timer, [124](#)
- MAC authentication user account format, [124](#)
- mGRE, [589](#), [592](#), [594](#)
- mGRE (full-mesh NAT traversal), [612](#)
- mGRE (full-mesh), [594](#), [601](#)
- mGRE (NHS-NHC), [598](#), [607](#)
- mGRE tunnel, [592](#)
- NAS-ID profile, [57](#)
- NETCONF-over-SSH, [453](#)
- NETCONF-over-SSH client user line, [397](#)
- object group, [493](#)
- object policy, [495](#), [499](#)
- password control, [225](#), [228](#), [232](#)
- PKI, [245](#), [248](#), [259](#)
- PKI certificate import/export, [275](#)
- PKI certificate request (automatic), [252](#)
- PKI certificate request (manual), [252](#)
- PKI certificate request abort, [253](#)
- PKI certificate-based access control policy, [257](#), [274](#)
- PKI domain, [249](#)
- PKI entity, [248](#)
- PKI Keon CA server certificate request (NAT-PT network), [268](#)
- PKI OpenCA server certificate request, [265](#)
- PKI RSA Keon CA server certificate request, [259](#)
- PKI Windows 2003 CA server certificate request, [261](#)

- PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)
- port object group, [494](#)
- port security, [202](#), [205](#), [213](#)
- port security client
- macAddressElseUserLoginSecure, [218](#)
- port security client userLoginWithOUI, [215](#)
- port security features, [208](#)
- port security intrusion protection, [208](#)
- port security MAC address autoLearn, [213](#)
- port security NTK feature, [208](#)
- port security secure MAC addresses, [209](#)
- preauthentication IP address pool for portal user, [148](#)
- public peer key, [239](#)
- routing for mGRE, [593](#)
- Secure Telnet client user line, [397](#)
- security portal authentication, [134](#), [139](#), [157](#)
- security portal authentication (cross-subnet for MPLS L3VPN), [192](#)
- security portal authentication cross-subnet, [170](#)
- security portal authentication destination subnet, [145](#)
- security portal authentication detection features, [149](#)
- security portal authentication direct, [157](#)
- security portal authentication direct with preauthentication domain, [194](#)
- security portal authentication extended cross-subnet, [180](#)
- security portal authentication extended direct, [173](#)
- security portal authentication extended re-DHCP, [176](#)
- security portal authentication fail-permit, [153](#)
- security portal authentication portal-free rule, [143](#)
- security portal authentication re-DHCP, [167](#)
- security portal authentication re-DHCP with preauthentication domain, [196](#)
- security portal authentication server, [140](#)
- security portal authentication server BAS-IP, [153](#)

- security portal authentication server detection, [150](#)
- security portal authentication server detection+user synchronization, [184](#)
- security portal authentication source subnet, [144](#)
- security portal authentication user online detection, [149](#)
- security portal authentication user synchronization, [152](#)
- security portal authentication Web server, [141](#)
- security portal authentication Web server detection, [151](#)
- service object group, [494](#)
- session management, [479](#), [480](#)
- session management logging, [482](#)
- SSH, [392](#)
- SSH client host public key, [398](#)
- SSH device as Secure Telnet client, [402](#)
- SSH device as server, [395](#)
- SSH device as SFTP client, [406](#)
- SSH management parameters, [400](#)
- SSH SCP, [444](#)
- SSH SCP (Suite B), [446](#)
- SSH SCP client device, [411](#)
- SSH SCP file+password authentication, [444](#)
- SSH Secure Telnet, [417](#)
- SSH Secure Telnet (128-bit Suite B), [431](#)
- SSH Secure Telnet client password authentication, [425](#)
- SSH Secure Telnet client publickey authentication, [429](#)
- SSH Secure Telnet server password authentication, [417](#)
- SSH Secure Telnet server publickey authentication, [420](#)
- SSH SFTP, [435](#)
- SSH SFTP (192-bit Suite B), [440](#)
- SSH SFTP client publickey authentication, [437](#)

- SSH SFTP server password authentication, [435](#)
- SSH user, [399](#)
- SSH2 algorithms (encryption ), [416](#)
- SSH2 algorithms (key exchange), [415](#)
- SSH2 algorithms (MAC), [416](#)
- SSH2 algorithms (public key), [416](#)
- SSL, [455](#), [456](#)
- SSL client policy, [458](#)
- SSL server policy, [456](#), [459](#)
- uRPF, [564](#), [568](#), [569](#)
- user profile, [223](#), [224](#)
- Web redirect, [155](#)

#### connecting

- connection limit. See [connection limit](#)

#### connection limit

- configuration, [486](#), [489](#)
- configuration (interface-based), [486](#)
- display, [488](#)
- maintain, [488](#)
- policy application, [488](#)
- policy configuration, [487](#)
- policy creation, [487](#)
- troubleshoot overlapping ACL segments, [491](#)

#### connection limits

- troubleshoot, [491](#)

#### consistency check (ARP attack protection), [551](#)

#### controlling

- 802.1X controlled/uncontrolled port, [79](#)
- AAA RADIUS session-control, [54](#)
- port security MAC address learning, [203](#)
- security portal authentication user access, [143](#)

#### cookie challenging

- IPsec IKEv2, [364](#)
- IPsec IKEv2 cookie challenging, [371](#)

#### copying

- IPsec packet DF bit copy, [307](#)

#### creating

- AAA HWTACACS scheme, [36](#)
- AAA ISP domain, [46](#)

- AAA LDAP scheme, [45](#)
- AAA RADIUS scheme, [26](#)
- attack D&P defense policy, [511](#)
- connection limit policy, [487](#)
- IPv4 object policy, [496](#)
- IPv6 object policy, [496](#)
- local key pair, [236](#)
- security LDAP server, [42](#)
- critical VLAN
  - 802.1X authentication, [91](#)
  - 802.1X configuration, [103](#)
- CRL
  - PKI, [245](#)
  - PKI architecture, [246](#)
  - PKI CA policy, [246](#)
  - PKI certificate export, [256](#)
  - PKI certificate removal, [257](#)
  - PKI certificate-based access control policy, [257](#)
  - troubleshooting PKI CRL obtain failure, [283](#)
- cross-subnet
  - portal authentication, [170](#)
  - portal authentication (MPLS L3VPN), [192](#)
  - portal authentication extended, [180](#)
  - portal authentication mode, [137](#), [137](#)
- crypto engine
  - configuration, [577](#)
  - display, [578](#)
  - hardware configuration, [577](#)
  - IPsec, [289](#)
  - maintain, [578](#)
- cryptography
  - FIPS self-test, [583](#)
- D**
- DAE
  - AAA RADIUS DAE server, [55](#)
- data
  - SSL configuration, [455](#), [456](#)

- data encryption
  - PKI configuration, [245](#), [248](#), [259](#)
- DDoS attack (uRPF), [564](#)
- default
  - IPv6 uRPF default route, [571](#)
  - uRPF route, [564](#)
- defending
  - attack D&P defense policy, [511](#)
  - attack D&P defense policy (flood), [513](#)
  - attack D&P defense policy (scanning), [513](#)
  - attack D&P defense policy (single-packet), [511](#)
  - attack D&P defense policy configuration (ACK flood), [514](#)
  - attack D&P defense policy configuration (DNS flood), [517](#)
  - attack D&P defense policy configuration (FIN flood), [515](#)
  - attack D&P defense policy configuration (HTTP flood), [518](#)
  - attack D&P defense policy configuration (ICMP flood), [516](#)
  - attack D&P defense policy configuration (ICMPv6 flood), [516](#)
  - attack D&P defense policy configuration (RST flood), [515](#)
  - attack D&P defense policy configuration (SYN flood), [514](#)
  - attack D&P defense policy configuration (SYN-ACK flood), [514](#)
  - attack D&P defense policy configuration (UDP flood), [517](#)
  - attack D&P policy application (device), [519](#)
  - attack D&P policy application (interface), [519](#)
- delaying
  - MAC authentication delay, [125](#)
- delimiter (802.1X domain name), [103](#)
- DES
  - IPsec encryption algorithm, [288](#)
- describing
  - object policy rule description, [495](#)

- destination
  - security portal authentication portal-free rule, [143](#)
  - security portal authentication subnet, [145](#)
- destroying
  - local key pair, [238](#)
- detecting
  - AAA RADIUS server status detection test profile, [25](#)
  - ARP attack detection (source MAC-based), [549](#), [550](#)
  - ARP detection configuration, [554](#)
  - attack D&P detection exemption, [518](#)
  - security portal authentication detection features, [149](#)
  - security portal authentication server, [150](#)
  - security portal authentication server detection+user synchronization, [184](#)
  - security portal authentication user online detection, [149](#)
  - security portal authentication user synchronization, [152](#)
  - security portal authentication Web server, [151](#)
- device
  - 802.1X authentication, [83](#)
  - 802.1X authentication configuration, [106](#)
  - 802.1X authentication initiation, [82](#)
  - 802.1X authorization VLAN assignment configuration, [108](#)
  - 802.1X basic configuration, [106](#)
  - 802.1X configuration, [88](#), [95](#)
  - 802.1X EAD assistant, [104](#)
  - 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
  - 802.1X EAD assistant configuration (DHCP server), [115](#)
  - 802.1X guest VLAN assignment configuration, [108](#)
  - 802.1X SmartOn, [105](#)
  - 802.1X SmartOn feature configuration, [117](#)

- 802.1X+ACL assignment configuration, [111](#)
- AAA configuration, [1](#), [18](#), [58](#)
- AAA device management user, [20](#)
- AAA HWTACACS accounting server, [37](#)
- AAA HWTACACS authentication server, [36](#)
- AAA HWTACACS authorization server, [37](#)
- AAA HWTACACS implementation, [7](#)
- AAA HWTACACS scheme, [36](#)
- AAA HWTACACS scheme VPN, [38](#)
- AAA HWTACACS shared keys, [38](#)
- AAA implementation, [12](#)
- AAA LDAP attribute map for authorization, [45](#)
- AAA LDAP authentication server, [45](#)
- AAA LDAP authorization server, [45](#)
- AAA LDAP implementation, [9](#)
- AAA LDAP scheme, [42](#)
- AAA LDAP server timeout period, [43](#)
- AAA local user, [20](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA RADIUS accounting server parameters, [27](#)
- AAA RADIUS authentication server, [26](#)
- AAA RADIUS implementation, [2](#)
- AAA RADIUS scheme, [25](#)
- AAA RADIUS scheme VPN, [28](#)
- AAA RADIUS security policy server IP address, [33](#)
- AAA RADIUS server status, [29](#)
- AAA RADIUS shared keys, [28](#)
- AAA scheme, [19](#)
- APR configuration, [478](#)
- attack D&P blacklist configuration, [531](#)
- attack D&P client verification configuration (DNS), [533](#)
- attack D&P client verification configuration (HTTP), [534](#)
- attack D&P client verification configuration (TCP), [532](#)
- attack D&P configuration, [503](#), [511](#), [528](#)
- attack D&P configuration (interface-based), [528](#)

- attack D&P defense policy, [511](#)
- attack D&P device-preventable attacks, [503](#)
- attack D&P policy application (device), [519](#)
- authorized ARP (DHCP server), [552](#)
- connection limit configuration, [486](#), [489](#)
- connection limit configuration (interface-based), [486](#)
- crypto engine configuration, [577](#)
- crypto engine hardware configuration, [577](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- MAC authentication, [120](#), [123](#), [127](#)
- MAC authentication (local), [127](#)
- MAC authentication (RADIUS-based), [129](#)
- MAC authentication ACL assignment, [131](#)
- MAC authentication configuration, [120](#)
- password control configuration, [225](#), [228](#), [232](#)
- password control parameters (global), [229](#)
- password control parameters (local user), [231](#)
- password control parameters (super), [231](#)
- password control parameters (user group), [230](#)
- password setting, [225](#)
- port security server authorization information, [211](#)
- portal authentication direct configuration, [157](#)
- portal authentication re-DHCP, [167](#)
- security portal authentication AAA server, [135](#)
- security portal authentication client, [135](#)
- security portal authentication configuration, [157](#)
- security portal authentication device access, [135](#)
- security portal authentication policy server, [135](#)
- security portal authentication server, [135](#)
- security portal authentication Web server, [135](#)
- SSH SCP client, [411](#)
- SSH SCP server enable, [397](#)

- SSH Secure Telnet client, [402](#)
- SSH Secure Telnet configuration (128-bit Suite B), [431](#)
- SSH Secure Telnet server connection establishment, [403](#)
- SSH Secure Telnet server connection establishment based on Suite B, [406](#)
- SSH Secure Telnet server enable, [396](#)
- SSH server configuration, [395](#)
- SSH SFTP client, [406](#)
- SSH SFTP configuration (192-bit Suite B), [440](#)
- SSH SFTP server enable, [396](#)
- SSL server policy configuration, [456](#), [459](#)
- uRPF configuration, [569](#)
- user profile, [224](#)
- user profile configuration, [223](#)

#### DF bit

- IPsec packet DF bit clear, [307](#)
- IPsec packet DF bit copy, [307](#)
- IPsec packet DF bit set, [307](#)

#### DH algorithm

- IPsec IKE, [333](#)
- IPsec PFS, [333](#)

#### DH guessing

- IPsec IKEv2, [364](#)

#### DHCP

- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
- 802.1X EAD assistant configuration (DHCP server), [115](#)
- authorized ARP (DHCP server), [552](#)
- authorized ARP (relay agent), [553](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- security portal authentication extended re-DHCP configuration, [176](#)
- security portal authentication modes, [136](#)

- security portal authentication process, [137](#)
- security portal authentication re-DHCP configuration, [167](#), [196](#)
- security portal authentication re-DHCP process (with CHAP/PAP authentication), [138](#)
- troubleshooting security portal authentication users cannot log in (re-DHCP), [200](#)
- DHCPv6
  - IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- digital certificate
  - PKI CA certificate, [245](#)
  - PKI CA policy, [246](#)
  - PKI CA storage path, [256](#)
  - PKI certificate export, [256](#)
  - PKI certificate import/export, [275](#)
  - PKI certificate obtain, [253](#)
  - PKI certificate removal, [257](#)
  - PKI certificate request, [251](#)
  - PKI certificate request (automatic), [252](#)
  - PKI certificate request (manual), [252](#)
  - PKI certificate request abort, [253](#)
  - PKI certificate verification, [254](#)
  - PKI certificate-based access control policy, [257](#)
  - PKI configuration, [245](#), [248](#), [259](#)
  - PKI CRL, [245](#)
  - PKI domain configuration, [249](#)
  - PKI entity configuration, [248](#)
  - PKI Keon CA server certificate request (NAT-PT network), [268](#)
  - PKI local certificate, [245](#)
  - PKI OpenCA server certificate request, [265](#)
  - PKI peer certificate, [245](#)
  - PKI RA certificate, [245](#)
  - PKI RSA Keon CA server certificate request, [259](#)
  - PKI verification (CRL checking), [254](#)
  - PKI verification (w/o CRL checking), [255](#)
  - PKI Windows 2003 CA server certificate request, [261](#)
- Digital Signature Algorithm. Use [DSA](#)
- direct portal authentication mode, [136](#), [137](#)
- directory
  - AAA LDAP directory service, [9](#)
  - SSH SFTP, [410](#)
- disabling
  - attack D&P log aggregation, [520](#)
- displaying
  - 802.1X, [106](#)
  - AAA, [58](#)
  - AAA HWTACACS, [41](#)
  - AAA LDAP, [46](#)
  - AAA local users/user groups, [24](#)
  - AAA RADIUS, [35](#)
  - APR, [477](#)
  - ARP attack detection (source MAC-based), [549](#)
  - ARP attack protection (unresolvable IP attack), [547](#)
  - ARP detection, [557](#)
  - ASPF, [467](#)
  - attack D&P, [523](#)
  - connection limit, [488](#)
  - crypto engine, [578](#)
  - FIPS, [584](#)
  - host public key, [238](#)
  - IP source guard (IPSG), [539](#)
  - IPsec, [313](#)
  - IPsec IKE, [342](#)
  - IPsec IKEv2, [372](#)
  - IPv4 source guard (IPv4SG), [539](#)
  - IPv6 source guard (IPv6SG), [539](#)
  - IPv6 uRPF, [575](#)
  - MAC authentication, [127](#)
  - mGRE, [594](#)
  - object group, [494](#)
  - object policy, [499](#)
  - password control, [232](#)

- PKI, [258](#)
- port security, [213](#)
- public key, [240](#)
- security portal authentication, [156](#)
- session management, [483](#)
- SSH, [417](#)
- SSH SFTP help information, [411](#)
- SSL, [459](#)
- uRPF, [569](#)
- user profile, [224](#)

distributing

- local host public key, [237](#)

DNS

- attack D&P defense policy (DNS flood), [517](#)
- attack D&P DNS client verification, [509](#), [521](#)
- attack D&P DNS client verification configuration, [533](#)

domain

- 802.1X mandatory port authentication domain, [100](#)
- 802.1X supported domain name delimiters, [103](#)
- AAA ISP domain accounting method, [52](#)
- AAA ISP domain attribute, [47](#)
- AAA ISP domain authentication method, [49](#)
- AAA ISP domain authorization method, [51](#)
- MAC authentication, [123](#)
- PKI domain configuration, [249](#)
- security portal authentication domain, [146](#)
- security portal preauthentication domain, [147](#)

Don't Fragment bit. See [DF bit](#)

DoS attack (uRPF), [564](#)

DPD

- IPsec IKE DPD, [340](#)
- IPsec IKEv2 DPD, [371](#)

DSA

- IPsec IKE signature authentication, [332](#)
- public key management, [236](#), [240](#)
- SCP client DSA host key pair, [411](#)

- SFTP client DSA host key pair, [406](#)
- SSH client host public key configuration, [398](#)
- SSH Secure Telnet client publickey authentication, [429](#)
- SSH server DSA host key pair, [395](#)
- Stelnet client DSA host key pair, [402](#)

DSCP

- AAA RADIUS packet DSCP priority change, [55](#)

dst-mac validity check (ARP detection), [556](#)

dynamic

- IP source guard (IPSG) dynamic binding, [537](#)
- IPv4 source guard (IPv4SG) dynamic binding configuration, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)

**E**

EAD

- 802.1X EAD assistant, [93](#), [104](#)
- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
- 802.1X EAD assistant configuration (DHCP server), [115](#)
- troubleshooting security 802.1X EAD assistant Web browser users not correctly redirected, [119](#)

EAP

- 802.1X EAP over RADIUS, [81](#)
- 802.1X EAP relay enable, [96](#)
- 802.1X EAP termination enable, [96](#)
- 802.1X packet format, [80](#)
- 802.1X RADIUS EAP-Message attribute, [81](#)
- 802.1X RADIUS Message-Authentication attribute, [82](#)
- 802.1X relay authentication, [84](#)
- 802.1X relay termination, [86](#)
- 802.1X relay/termination authentication, [84](#)

EAPOL



- 802.1X authentication (access device initiated), [82](#)
- 802.1X authentication (client-initiated), [82](#)
- 802.1X packet format, [81](#)
- ECDSA
  - public key management, [236](#), [240](#)
- Elliptic Curve Digital Signature Algorithm.
- Use [ECDSA](#)
- email (PKI secure), [247](#)
- enabling
  - 802.1X, [95](#)
  - 802.1X EAP relay, [96](#)
  - 802.1X EAP termination, [96](#)
  - 802.1X periodic online user reauthentication, [101](#)
  - AAA RADIUS accounting-on, [32](#)
  - AAA RADIUS accounting-on (extended), [33](#)
  - AAA RADIUS session-control, [54](#)
  - AAA RADIUS SNMP notification, [35](#)
  - APR application statistics, [476](#)
  - IPsec ACL de-encapsulated packet check, [304](#)
  - IPsec IKE invalid SPI recovery, [340](#)
  - IPsec IKEv2 cookie challenging, [371](#)
  - IPsec packet logging, [307](#)
  - IPsec QoS pre-classify, [307](#)
  - IPv4 object policy rule matching acceleration, [498](#)
  - IPv4 source guard (IPv4SG) on interface, [538](#)
  - IPv6 object policy rule matching acceleration, [498](#)
  - IPv6 source guard (IPv6SG) on interface, [538](#)
  - MAC authentication, [123](#)
  - MAC authentication multi-VLAN mode, [126](#)
  - NETCONF-over-SSH, [397](#)
  - outgoing packets filtering on portal interface, [149](#)
  - password control, [228](#)
  - port security, [205](#)

- port security authorization-fail-offline, [212](#)
- port security MAC move, [211](#)
- security portal authentication, [141](#)
- security portal authentication roaming, [154](#)
- session management statistics collection, [482](#)
- SSH SCP server, [397](#)
- SSH Secure Telnet server, [396](#)
- SSH SFTP server, [396](#)
- strict-checking mode on portal authorization information, [148](#)
- encapsulating
  - 802.1X RADIUS EAP-Message attribute, [81](#)
  - IPsec ACL de-encapsulated packet check, [304](#)
  - IPsec anti-replay, [305](#)
  - IPsec configuration, [286](#), [314](#)
  - IPsec RIPng configuration, [324](#)
  - IPsec RRI configuration, [308](#), [327](#)
  - IPsec transport mode, [287](#)
  - IPsec tunnel for IPv4 packets (IKE-based), [317](#)
  - IPsec tunnel for IPv4 packets (manual), [314](#)
  - IPsec tunnel for IPv6 packets (IKE-based), [320](#)
  - IPsec tunnel mode, [287](#)
- encrypting
  - crypto engine configuration, [577](#)
  - crypto engine hardware configuration, [577](#)
  - IPsec, [288](#)
  - IPsec configuration, [286](#), [314](#)
  - IPsec crypto engine, [289](#)
  - IPsec encryption algorithm (3DES), [288](#)
  - IPsec encryption algorithm (AES), [288](#)
  - IPsec encryption algorithm (DES), [288](#)
  - IPsec RIPng configuration, [324](#)
  - IPsec RRI configuration, [308](#), [327](#)
  - IPsec tunnel for IPv4 packets (IKE-based), [317](#)
  - IPsec tunnel for IPv4 packets (manual), [314](#)
  - IPsec tunnel for IPv6 packets (IKE-based), [320](#)
  - peer public key entry, [240](#)
  - public key import from file, [242](#)
  - public key management, [236](#), [240](#)



- SSH configuration, [392](#)
- SSH server configuration, [395](#)
- SSL services, [455](#)
- entering
  - FIPS mode (automatic reboot), [580](#), [584](#)
  - FIPS mode (manual reboot), [580](#), [585](#)
  - peer public key, [239](#), [240](#)
- ESP
  - IPsec security protocol 50, [286](#)
- establishing
  - IPsec tunnel establishment, [291](#)
  - mGRE tunnel, [590](#)
  - SSH SCP server connection, [412](#)
  - SSH SCP server connection based on Suite B, [415](#)
  - SSH Secure Telnet server connection, [403](#)
  - SSH Secure Telnet server connection based on Suite B, [406](#)
  - SSH SFTP server connection, [407](#)
  - SSH SFTP server connection based on Suite B, [409](#)
- Ethernet
  - 802.1X overview, [79](#)
  - ARP attack protection configuration, [546](#)
- exempting
  - attack D&P detection exemption, [518](#)
- exiting
  - FIPS mode (automatic reboot), [582](#), [587](#)
  - FIPS mode (manual reboot), [582](#), [587](#)
- exporting
  - host public key, [238](#)
  - PKI certificate, [256](#)
  - PKI certificate import/export, [275](#)
  - troubleshooting PKI certificate export failure, [284](#)
- extending
  - security portal authentication extended cross-subnet configuration, [180](#)

- security portal authentication extended direct configuration, [173](#)
- security portal authentication extended re-DHCP configuration, [176](#)
- external
  - ASPF external interface, [462](#)
- F**
- fail-permit feature (portal), [153](#)
- feature and hardware compatibility
  - user profile, [223](#)
- Federal Information Processing Standard. Use [FIPS](#)
- file
  - peer public key import from file, [239](#)
  - public key import from file, [242](#)
  - SSH SCP file transfer+password authentication, [444](#)
  - SSH SFTP, [410](#)
- filtering
  - ARP packets, [562](#), [563](#)
  - attack D&P blacklist, [506](#)
  - outgoing packets filtering on portal interface, [149](#)
- FIN flood, [515](#)
- FIPS
  - configuration, [579](#), [584](#)
  - configuration restrictions, [579](#)
  - display, [584](#)
  - mode configuration, [580](#)
  - mode entry, [580](#)
  - mode entry (automatic reboot), [584](#)
  - mode entry (manual reboot), [585](#)
  - mode exit, [582](#)
  - mode exit (automatic reboot), [587](#)
  - mode exit (manual reboot), [587](#)
  - mode system changes, [581](#)
  - self-test, [583](#)
- FIPS compliance
  - AAA, [18](#)
  - IPsec, [291](#)

- IPsec IKE, [333](#)
- password control, [228](#)
- PKI, [248](#)
- public key, [236](#)
- SSH, [395](#)
- SSL, [456](#)
- firewall
  - ASPF application inspection (H.323), [470](#)
  - ASPF application inspection (TCP), [468](#)
  - ASPF configuration, [462](#), [465](#), [467](#)
  - ASPF configuration application inspection (FTP), [467](#)
- fixed ARP
  - configuration, [560](#)
  - configuration restrictions, [560](#)
- flood attack
  - attack D&P defense policy, [513](#)
  - attack D&P defense policy (ACK flood), [514](#)
  - attack D&P defense policy (DNS flood), [517](#)
  - attack D&P defense policy (FIN flood), [515](#)
  - attack D&P defense policy (HTTP flood), [518](#)
  - attack D&P defense policy (ICMP flood), [516](#)
  - attack D&P defense policy (ICMPv6 flood), [516](#)
  - attack D&P defense policy (RST flood), [515](#)
  - attack D&P defense policy (SYN flood), [514](#)
  - attack D&P defense policy (SYN-ACK flood), [514](#)
  - attack D&P defense policy (UDP flood), [517](#)
  - attack D&P device-preventable attacks, [503](#), [505](#)
- forcing
  - security portal authentication forced type, [134](#)
- format
  - 802.1X EAP packet format, [80](#)
  - 802.1X EAPOL packet format, [81](#)
  - 802.1X packet, [80](#)
  - AAA HWTACACS username, [39](#)
  - AAA RADIUS packet format, [3](#)
  - AAA RADIUS username, [28](#)
  - MAC authentication user account, [124](#)
  - specifying NAS-Port-ID attribute format, [154](#)
- forwarding
  - ARP detection restricted forwarding, [556](#), [558](#)
  - IP source guard (IPSG)
    - configuration, [536](#), [537](#), [540](#)
  - IPv4 source guard (IPv4SG) dynamic binding
    - configuration, [541](#)
  - IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
  - IPv4 source guard (IPv4SG) static binding
    - configuration, [540](#)
  - IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
  - IPv6 source guard (IPv6SG) static binding
    - configuration, [543](#)
  - mGRE packet forwarding, [591](#)
- fragment
  - attack D&P TCP fragment attack prevention, [520](#)
  - IPsec packet DF bit, [307](#)
- frame
  - port security configuration, [202](#), [205](#)
- FTP
  - AAA RADIUS Login-Service attribute check method, [34](#)
  - ASPF application inspection (FTP), [467](#)
  - local host public key distribution, [237](#)
  - SSH SCP server connection establishment, [412](#)
  - SSH SCP server connection establishment based on Suite B, [415](#)
  - SSH SFTP client device, [406](#)
  - SSH SFTP client publickey authentication, [437](#)
  - SSH SFTP configuration, [435](#)
  - SSH SFTP configuration (192-bit Suite B), [440](#)
  - SSH SFTP directories, [410](#)
  - SSH SFTP files, [410](#)
  - SSH SFTP packet source IP address, [407](#)
  - SSH SFTP server connection establishment, [407](#)

- SSH SFTP server connection establishment based on Suite B, [409](#)
- SSH SFTP server connection termination, [411](#)
- SSH SFTP server password authentication, [435](#)

#### full-mesh

- mGRE configuration, [594](#), [601](#)
- mGRE configuration (full-mesh NAT traversal), [612](#)
- mGRE network type, [590](#)

Fully Qualified Domain Name. *Use FQDN*

#### function

- security portal authentication extended functions, [134](#)

## G

#### gateway

- ARP gateway protection, [561](#), [561](#)
- IPsec RRI, [290](#)

#### generating

- SCP client local DSA key pair, [411](#)
- SCP client local RSA key pair, [411](#)
- SFTP client local DSA key pair, [406](#)
- SFTP client local RSA key pair, [406](#)
- SSH server local DSA key pair, [395](#)
- SSH server local RSA key pair, [395](#)
- Stelnet client local DSA key pair, [402](#)
- Stelnet client local RSA key pair, [402](#)

#### global

- IPsec IKE global identity information, [338](#)

#### global parameter

- IPsec IKEv2 global parameters, [371](#)

#### group

- APR (group-based), [474](#)
- APR application group configuration, [476](#)
- APR configuration, [478](#)
- APR configuration (group-based), [474](#)

#### guest VLAN

- 802.1X assignment configuration, [108](#)
- 802.1X authentication, [90](#)

- 802.1X configuration, [102](#)

## H

#### H.323

- ASPF application inspection (H.323), [470](#)

handshake protocol (SSL), [455](#)

#### handshaking

- 802.1X online user handshake, [99](#)

#### hardware

- attack D&P command and hardware compatibility, [503](#)
- crypto engine configuration, [577](#), [577](#)

#### Hewlett Packard Enterprise

- AAA RADIUS Hewlett Packard Enterprise proprietary attributes, [16](#)

#### history

- password history, [226](#)

#### host

- public key export, [238](#)
- SSH client host public key configuration, [398](#)

#### HTTP

- attack D&P defense policy (HTTP flood), [518](#)
- attack D&P HTTP client verification, [510](#), [522](#)
- attack D&P HTTP client verification configuration, [534](#)
- SSL configuration, [455](#), [456](#)

#### HUAWEI

- AAA version-based RADIUS attribute interpretation, [35](#)

HW Terminal Access Controller Access Control System. *Use HWTACACS*

#### HWTACACS

- AAA configuration, [1](#), [18](#), [58](#)
- AAA for PPP user, [75](#)
- AAA for SSH user, [63](#)
- AAA implementation, [7](#)
- AAA local user configuration, [20](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA scheme, [19](#)
- accounting server, [37](#)

- authentication server, [36](#)
- authorization server, [37](#)
- display, [41](#)
- HWTACACS/RADIUS differences, [7](#)
- maintain, [41](#)
- outgoing packet source IP address, [39](#)
- packet exchange process, [7](#)
- protocols and standards, [14](#)
- real-time accounting timer, [40](#)
- scheme configuration, [36](#)
- scheme creation, [36](#)
- scheme VPN, [38](#)
- server quiet timer, [40](#)
- server response timeout timer (response-timeout), [40](#)
- shared keys, [38](#)
- traffic statistics units, [39](#)
- troubleshooting, [78](#)
- username format, [39](#)

Hypertext Transfer Protocol. Use [HTTP](#)

## I

### ICMP

- attack D&P defense policy (ICMP flood), [516](#)
- attack D&P defense policy (ICMPv6 flood), [516](#)

### identity

- IPsec IKE global identity information, [338](#)

### ignoring

- port security server authorization information, [211](#)

### IKE, [331](#), See also [ISAKMP](#)

- configuration, [331](#), [333](#), [342](#)
- configuration (aggressive mode+NAT traversal), [353](#)
- configuration (aggressive mode+RSA signature authentication), [346](#)
- configuration (main mode/pre-shared key authentication), [342](#)
- configuring IPsec for mGRE tunnel, [593](#)

- DH algorithm, [333](#)
- display, [342](#)
- DPD configuration, [340](#)
- FIPS compliance, [333](#)
- global identity information, [338](#)
- identity authentication, [332](#)
- invalid SPI recovery, [340](#)
- IPsec negotiation mode, [288](#)
- IPsec policy (IKE-based), [299](#)
- IPsec policy (IKE-based/direct), [300](#)
- IPsec policy (IKE-based/template), [301](#)
- IPsec profile (IKE-based), [311](#)
- IPsec SA, [288](#)
- IPsec tunnel establishment, [291](#)
- IPsec tunnel for IPv4 packets (IKE-based), [317](#)
- IPsec tunnel for IPv6 packets (IKE-based), [320](#)
- keepalive function, [339](#)
- keychain configuration, [337](#)
- maintain, [342](#)
- mGRE configuration (full-mesh), [601](#)
- mGRE configuration (NHS-NHC), [607](#)
- NAT keepalive function, [339](#)
- negotiation, [331](#)
- PFS, [333](#)
- profile configuration, [334](#)
- proposal configuration, [336](#)
- protocols and standards, [333](#)
- SA max, [341](#)
- security mechanism, [332](#)
- SNMP notification, [341](#)
- troubleshoot negotiation failure (no proposal match), [358](#)
- troubleshoot negotiation failure (no proposal or keychain specified correctly), [358](#)
- troubleshooting, [358](#)

IKEv2, [363](#), See also [ISAKMP](#)

- address pool, [372](#)
- configuration, [363](#), [364](#), [373](#)
- configuration (NAT traversal), [385](#)

- configuration (pre-shared key authentication), [373](#)
- configuration (RSA signature authentication), [377](#)
- cookie challenging, [364](#), [371](#)
- DH guessing, [364](#)
- display, [372](#)
- DPD configuration, [371](#)
- global parameter configuration, [371](#)
- keychain configuration, [370](#)
- maintain, [372](#)
- NAT keepalive, [372](#)
- negotiation, [363](#)
- new features, [364](#)
- policy configuration, [368](#)
- profile configuration, [365](#)
- proposal configuration, [369](#)
- protocols and standards, [364](#)
- retransmission, [364](#)
- SA rekeying, [364](#)
- troubleshoot, [390](#)
- troubleshoot negotiation failure (no proposal match), [390](#)

IKEv2 feature

- IPsec IKEv2 cookie challenging, [364](#)
- IPsec IKEv2 DH guessing, [364](#)
- IPsec IKEv2 retransmission, [364](#)
- IPsec IKEv2 SA rekeying, [364](#)

IMC

- AAA RADIUS session-control, [54](#)

implementing

- 802.1X MAC-based access control, [88](#)
- 802.1X port-based access control, [88](#)
- AAA for MPLS L3VPNs, [14](#)
- AAA HWTACACS, [7](#)
- AAA LDAP, [9](#)
- AAA on device, [12](#)
- AAA RADIUS, [2](#)
- IPsec, [289](#)
- IPsec ACL-based implementation, [289](#)
- IPsec application-based implementation, [290](#)
- security ACL-based IPsec, [292](#)

importing

- peer public key from file, [239](#)
- PKI certificate import/export, [275](#)
- public key from file, [242](#)
- troubleshooting PKI CA certificate import failure, [283](#)
- troubleshooting PKI local certificate import failure, [284](#)

initiating

- 802.1X authentication, [82](#), [83](#)

injecting

- IPsec RRI, [290](#)
- IPsec RRI configuration, [308](#)

Intelligent Target Accounting. *See* [ITA](#)

interface

- connection limit configuration, [486](#)
- portal outgoing packets filtering, [149](#)
- security portal authentication Web server reference, [142](#)

internal

- ASPF internal interface, [462](#)

Internet

- SSL configuration, [455](#), [456](#)

Internet Key Exchange. *Use* [IKE](#)

interpreting

- AAA HUAWEI RADIUS attributes 26-1 and 26-4 (version 1.0), [35](#)
- AAA HUAWEI RADIUS attributes 26-1 and 26-4 (version 1.1), [35](#)
- AAA RADIUS class attribute as CAR parameter, [33](#)

intrusion detection/protection

- session management, [479](#)
- session management configuration, [480](#)

intrusion protection

- port security blockmac mode, [208](#)

port security disableport mode, [208](#)

port security disableport-temporarily mode, [208](#)

port security feature, [202](#)

## IP

ARP attack protection (unresolvable IP attack), [547](#), [548](#)

ARP attack protection blackhole routing (unresolvable IP attack), [547](#)

ARP attack protection source suppression (unresolvable IP attack), [547](#)

ARP detection ip validity check, [556](#)

security. *Use* [IPsec](#)

uRPF configuration, [564](#), [568](#), [569](#)

## IP address pool

configuring preauthentication IP address pool for portal user, [148](#)

## IP addressing

AAA HWTACACS outgoing packet source IP address, [39](#)

AAA LDAP server IP address, [42](#)

AAA RADIUS outgoing packet source IP address, [30](#)

AAA RADIUS security policy server IP address, [33](#)

APR PBAR host port mapping (IP address-based), [474](#)

ARP attack protection configuration, [546](#)

ARP detection restricted forwarding, [558](#)

ARP detection user+packet validity check, [557](#)

ARP filtering configuration, [563](#)

ARP gateway protection, [561](#)

attack D&P blacklist, [506](#), [522](#)

authorized ARP (DHCP relay agent), [553](#)

authorized ARP (DHCP server), [552](#)

SSH Secure Telnet packet source IP address, [402](#)

SSH SFTP packet source IP address, [407](#)

## IP source guard

IPv4. *See* [IPv4 source guard](#)

IPv6. *See* [IPv6 source guard](#)

## IP source guard (IPSG)

configuration, [536](#), [537](#), [540](#)

display, [539](#)

dynamic binding, [537](#)

maintain, [539](#)

static binding, [536](#)

## IPoE

user profile configuration, [223](#)

## IPsec

ACL configuration, [292](#)

ACL de-encapsulated packet check, [304](#)

ACL IPsec anti-replay, [305](#)

ACL rule keywords, [292](#)

ACL-based implementation, [292](#)

ACL-based IPsec, [289](#)

anti-replay redundancy, [305](#)

application-based IPsec, [290](#)

authentication, [288](#)

authentication algorithms, [288](#)

configuration, [286](#), [314](#)

configuring IPsec for mGRE tunnel, [593](#)

crypto engine, [289](#)

display, [313](#)

encapsulation modes, [286](#)

encryption, [288](#)

encryption algorithms, [288](#)

FIPS compliance, [291](#)

IKE configuration, [331](#), [333](#), [342](#)

IKE configuration (aggressive mode+NAT traversal), [353](#)

IKE configuration (aggressive mode+RSA signature authentication), [346](#)

IKE configuration (main mode/pre-shared key authentication), [342](#)

IKE DPD, [340](#)

IKE global identity information, [338](#)

IKE identity authentication, [332](#)

- IKE invalid SPI recovery, [340](#)
- IKE keepalive function, [339](#)
- IKE keychain, [337](#)
- IKE NAT keepalive function, [339](#)
- IKE negotiation, [331](#)
- IKE negotiation mode, [288](#)
- IKE profile configuration, [334](#)
- IKE proposal, [336](#)
- IKE SA max, [341](#)
- IKE security mechanism, [332](#)
- IKE SNMP notification, [341](#)
- IKE-based profile application to tunnel interface, [312](#)
- IKEv2 address pool, [372](#)
- IKEv2 configuration, [363](#), [364](#), [373](#)
- IKEv2 configuration (NAT traversal), [385](#)
- IKEv2 configuration (pre-shared key authentication), [373](#)
- IKEv2 configuration (RSA signature authentication), [377](#)
- IKEv2 cookie challenging, [371](#)
- IKEv2 DPD, [371](#)
- IKEv2 global parameters, [371](#)
- IKEv2 keychain, [370](#)
- IKEv2 NAT keepalive, [372](#)
- IKEv2 negotiation, [363](#)
- IKEv2 new features, [364](#)
- IKEv2 policy configuration, [368](#)
- IKEv2 profile configuration, [365](#)
- IKEv2 proposal, [369](#)
- implementation, [289](#)
- IPv6. See [IPv6 IPsec](#)
- maintain, [313](#)
- mGRE configuration (full-mesh), [601](#)
- mGRE configuration (NHS-NHC), [607](#)
- mirror image ACLs, [294](#)
- non-mirror image ACLs, [294](#)
- packet DF bit, [307](#)
- packet logging enable, [307](#)

- PKI configuration, [245](#), [248](#), [259](#)
- policy application to interface, [303](#)
- policy configuration (IKE-based), [299](#)
- policy configuration (IKE-based/direct), [300](#)
- policy configuration (IKE-based/template), [301](#)
- policy configuration (manual), [297](#)
- policy configuration restrictions, [297](#)
- policy configuration restrictions (IKE-based), [299](#)
- profile configuration (IKE-based), [311](#)
- protocols and standards, [291](#)
- QoS pre-classify enable, [307](#)
- RIPng configuration, [324](#)
- RRI, [290](#)
- RRI configuration, [308](#), [327](#)
- SA, [288](#)
- security protocols, [286](#)
- security strength, [291](#)
- SNMP notification configuration, [312](#)
- source interface policy bind, [306](#)
- transform set, [295](#)
- troubleshoot IKE, [358](#)
- troubleshoot IKE negotiation failure (no proposal match), [358](#)
- troubleshoot IKE negotiation failure (no proposal or keychain specified correctly), [358](#)
- troubleshoot IKEv2, [390](#)
- troubleshoot IKEv2 negotiation failure (no proposal match), [390](#)
- troubleshoot SA negotiation failure (invalid identity info), [359](#)
- troubleshoot SA negotiation failure (no transform set match), [359](#), [390](#)
- troubleshoot SA negotiation failure (tunnel failure), [391](#)
- tunnel configuration, [311](#)
- tunnel establishment, [291](#)
- tunnel for IPv4 packets (IKE-based), [317](#)
- tunnel for IPv4 packets (manual), [314](#)
- tunnel for IPv6 packets (IKE-based), [320](#)



## IPv4

- address object group, [493](#)
- address object group configuration, [493](#)
- IPsec tunnel for IPv4 packets (IKE-based), [317](#)
- IPsec tunnel for IPv4 packets (manual), [314](#)
- object policy creation, [496](#)
- object policy rule configuration, [496](#)
- object policy rule match order change, [498](#)
- object policy rule matching acceleration, [498](#)
- object policy zone pair application, [498](#)
- source guard. See IPv4 source guard
- SSH SCP client device, [411](#)
- SSH SCP server connection establishment, [412](#)
- SSH SCP server connection establishment based on Suite B, [415](#)
- SSH Secure Telnet server connection establishment, [403](#)
- SSH Secure Telnet server connection establishment based on Suite B, [406](#)
- SSH SFTP server connection establishment, [407](#)
- SSH SFTP server connection establishment based on Suite B, [409](#)

## IPv4 source guard (IPv4SG)

- configuration, [536](#), [537](#), [537](#), [540](#)
- display, [539](#)
- dynamic binding configuration, [541](#)
- dynamic binding+DHCP relay configuration, [542](#)
- enable on interface, [538](#)
- maintain, [539](#)
- static binding configuration, [538](#), [540](#)

## IPv6

- address object group, [493](#)
- address object group configuration, [493](#)
- IPsec. See [IPv6 IPsec](#)
- IPsec tunnel for IPv6 packets (IKE-based), [320](#)

- object policy creation, [496](#)
- object policy rule configuration, [496](#)
- object policy rule match order change, [498](#)
- object policy rule matching acceleration, [498](#)
- object policy zone pair application, [498](#)
- source guard. See IPv6 source guard
- SSH SCP client device, [411](#)
- SSH SCP server connection establishment, [412](#)
- SSH SCP server connection establishment based on Suite B, [415](#)
- SSH Secure Telnet server connection establishment, [403](#)
- SSH Secure Telnet server connection establishment based on Suite B, [406](#)
- SSH SFTP server connection establishment, [407](#)
- SSH SFTP server connection establishment based on Suite B, [409](#)
- uRPF. See [IPv6 uRPF](#)

## IPv6 IPsec

- routing protocol profile (manual), [309](#)
- routing protocols configuration, [309](#)

## IPv6 source guard (IPv6SG)

- configuration, [536](#), [537](#), [538](#), [540](#)
- display, [539](#)
- dynamic binding+DHCPv6 snooping configuration, [544](#)
- enable on interface, [538](#)
- maintain, [539](#)
- static binding configuration, [539](#), [543](#)

## IPv6 uRPF

- check modes, [571](#)
- command and hardware compatibility, [574](#)
- configuration, [571](#), [574](#), [575](#)
- display, [575](#)
- features, [571](#)
- network application, [574](#)
- operation, [572](#)

## ISAKAMP

- protocols and standards, [333](#), [364](#)



ISAKMP, [331](#), [363](#), *See also* [IKE](#)

IPsec IKE configuration, [331](#), [333](#), [342](#)

IPsec IKE configuration (aggressive mode+NAT traversal), [353](#)

IPsec IKE configuration (aggressive mode+RSA signature authentication), [346](#)

IPsec IKE configuration (main mode/pre-shared key authentication), [342](#)

IPsec IKEv2 configuration, [363](#), [364](#), [373](#)

IPsec IKEv2 configuration (NAT traversal), [385](#)

IPsec IKEv2 configuration (pre-shared key authentication), [373](#)

IPsec IKEv2 configuration (RSA signature authentication), [377](#)

## ISP

AAA device implementation, [12](#)

AAA ISP domain accounting method, [52](#)

AAA ISP domain attribute, [47](#)

AAA ISP domain authentication method, [49](#)

AAA ISP domain authorization method, [51](#)

AAA ISP domain creation, [46](#)

AAA ISP domain method, [46](#)

## ITA

AAA ITA policy configuration, [56](#)

## K

### keepalive

IPsec IKE function, [339](#)

IPsec IKE NAT function, [339](#)

IPsec IKEv2 NAT, [372](#)

keep-online feature (MAC authentication), [126](#)

### Keon CA

PKI CA server certificate request (NAT-PT network), [268](#)

### key

IPsec IKE pre-shared key authentication, [332](#)

PKI configuration, [245](#), [248](#), [259](#)

### key pair

SCP client DSA host key pair, [411](#)

SCP client RSA host key pair, [411](#)

SCP client RSA server key pair, [411](#)

SFTP client DSA host key pair, [406](#)

SFTP client RSA host key pair, [406](#)

SFTP client RSA server key pair, [406](#)

SSH server DSA host key pair, [395](#)

SSH server RSA host key pair, [395](#)

SSH server RSA server key pair, [395](#)

Stelnet client DSA host key pair, [402](#)

Stelnet client RSA host key pair, [402](#)

Stelnet client RSA server key pair, [402](#)

### keychain

IPsec IKE keychain, [337](#)

IPsec IKEv2 keychain, [370](#)

### keyword

IPsec ACL rule keywords, [292](#)

## L

### LAN

802.1X overview, [79](#)

### Layer 3

IPsec configuration, [286](#), [314](#)

IPsec RIPng configuration, [324](#)

IPsec RRI configuration, [308](#), [327](#)

IPsec tunnel for IPv4 packets (IKE-based), [317](#)

IPsec tunnel for IPv4 packets (manual), [314](#)

IPsec tunnel for IPv6 packets (IKE-based), [320](#)

PKI MPLS L3VPN support, [247](#)

### LDAP

AAA configuration, [1](#), [18](#), [58](#)

AAA implementation, [9](#)

AAA LDAP server SSH user authentication, [65](#)

AAA LDAP server SSL VPN user authentication+authorization, [70](#)

AAA local user configuration, [20](#)

AAA scheme, [19](#)

administrator attribute, [43](#)

attribute map, [44](#)

attribute map for authorization, [45](#)

- authentication, 9
- authentication process, 10
- authentication server, 45
- authorization, 9
- authorization process, 11
- authorization server, 45
- directory service, 9
- display, 46
- protocols and standards, 14
- scheme configuration, 42
- scheme creation, 45
- server creation, 42
- server IP address, 42
- server timeout period, 43
- troubleshooting user authentication fails, 78
- user attribute, 43
- versions, 42

learning

- mGRE route learning, 591

Lightweight Directory Access Protocol. *Use* [LDAP](#)

limiting

- connection limit. *See* [connection limit](#)
- port security secure MAC addresses, 206

link

- uRPF link layer check, 564

local

- 802.1X authorization VLAN, 88
- AAA local accounting method, 13
- AAA local authentication, 13
- AAA local authentication configuration, 18
- AAA local authorization method, 13
- AAA SSH user
- authentication+authorization, 62
- host public key display, 238
- host public key distribution, 237
- host public key export, 238
- key pair creation, 236
- key pair destruction, 238
- MAC authentication, 120

- MAC authentication (local), 127
- password control parameters (local user), 231
- PKI digital certificate, 245
- troubleshooting PKI certificate obtain failure, 281
- troubleshooting PKI certificate request failure, 282
- troubleshooting PKI local certificate import failure, 284

log aggregation, 520

logging

- attack D&P log aggregation, 520
- IPsec packet logging enable, 307
- password events, 227
- session management logging, 482

logging in

- AAA concurrent login user max, 56
- password expired login, 226
- password user first login, 227
- password user login attempt limit, 227
- password user login control, 227
- RADIUS Login-Service attribute, 34

logging out

- security portal authentication users, 155

## M

### MAC

- 802.1X MAC-based access control, 88
- address. *See* [MAC addressing](#)
- ARP attack detection (source MAC-based), 549
- authentication. *See* [MAC authentication](#)
- SSL services, 455

### MAC address

- 802.1X authentication (client-initiated), 82

### MAC addressing

- 802.1X authentication (access device initiated), 82
- ARP attack detection (source MAC-based), 550
- ARP attack protection configuration, 546
- ARP packet source MAC consistency check, 551

- IP source guard (IPSG)
  - configuration, [536](#), [537](#), [540](#)
- IPv4 source guard (IPv4SG) dynamic binding
  - configuration, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv4 source guard (IPv4SG) static binding
  - configuration, [540](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- IPv6 source guard (IPv6SG) static binding
  - configuration, [543](#)
- MAC authentication, [123](#), [127](#)
- MAC authentication (local), [127](#)
- MAC authentication (RADIUS-based), [129](#)
- MAC authentication configuration, [120](#)
- port security client
  - macAddressElseUserLoginSecure, [218](#)
  - port security MAC address autoLearn, [213](#)
  - port security macAddressWithRadius, [204](#)
  - port security secure MAC address, [209](#)
  - port security secure MAC address port limit, [206](#)
  - troubleshooting port security secure MAC addresses, [222](#)
- MAC authentication
  - ACL assignment, [121](#), [131](#)
  - concurrent port users max, [125](#)
  - configuration, [120](#), [123](#), [127](#)
  - delay configuration, [125](#)
  - display, [127](#)
  - domain specification, [123](#)
  - enable, [123](#)
  - keep-online, [126](#)
  - local authentication, [120](#), [127](#)
  - maintain, [127](#)
  - multi-VLAN mode configuration, [126](#)
  - periodic reauthentication, [121](#)
  - port security authentication control mode, [202](#)
  - port security client
    - macAddressElseUserLoginSecure, [218](#)
    - port security client userLoginWithOUI, [215](#)
    - port security configuration, [202](#), [205](#), [213](#)
    - port security features, [208](#)
    - port security intrusion protection, [208](#)
    - port security MAC address autoLearn, [213](#)
    - port security MAC move, [211](#)
    - port security MAC+802.1X authentication, [204](#)
    - port security mode, [206](#)
    - port security NTK, [208](#)
    - RADIUS-based, [120](#), [129](#)
    - timer configuration, [124](#)
    - user account format, [124](#)
    - user account policies, [120](#)
    - VLAN assignment, [121](#)
- MAC learning
  - port security autoLearn MAC learning control, [203](#)
  - port security MAC learning control modes, [202](#)
  - port security secure MAC learning control, [203](#)
- maintaining
  - 802.1X, [106](#)
  - AAA HWTACACS, [41](#)
  - AAA RADIUS, [35](#)
  - APR, [477](#)
  - ARP detection, [557](#)
  - ASPF, [467](#)
  - attack D&P, [523](#)
  - connection limit, [488](#)
  - crypto engine, [578](#)
  - IP source guard (IPSG), [539](#)
  - IPsec, [313](#)
  - IPsec IKE, [342](#)
  - IPsec IKEv2, [372](#)
  - IPv4 source guard (IPv4SG), [539](#)
  - IPv6 source guard (IPv6SG), [539](#)
  - MAC authentication, [127](#)
  - mGRE, [594](#)
  - password control, [232](#)

- security portal authentication, 156
- session management, 483
- managing
  - public keys, 236, 240
  - sessions. *See* session management
- manual
  - FIPS mode (manual reboot), 580
  - FIPS mode entry (manual reboot), 585
  - FIPS mode exit (manual reboot), 582, 587
  - IPsec IPv6 routing protocol profile (manual), 309
- mapping
  - APR configuration, 474, 478
  - APR PBAR configuration, 475
  - APR PBAR general port mapping, 474
  - APR PBAR host port mapping, 474
- matching
  - object policy rule match order, 495
  - object policy rule match order change, 498
  - object policy rule matching acceleration, 498
- message
  - ARP attack protection configuration, 546
- Message Authentication Code. *Use* MAC
- mGRE
  - configuration, 589, 592, 594
  - display, 594
  - full-mesh configuration, 594, 601
  - full-mesh NAT traversal configuration, 612
  - IPsec for mGRE tunnel configuration, 593
  - maintain, 594
  - NAT traversal, 592
  - network type, 590
  - NHC, 589
  - NHS, 589
  - NHS-NHC configuration, 598, 607
  - operation procedure, 589
  - operation scheme, 589
  - overview, 589
  - packet forwarding, 591
  - registration, 589
  - route learning, 591
  - routing configuration, 593
  - tunnel configuration, 592
  - tunnel establishment, 590
- minimum password length, 225
- mirroring
  - IPsec mirror image ACLs, 294
  - IPsec non-mirror image ACLs, 294
- mode
  - 802.1X EAP relay/termination comparison, 84
  - 802.1X multicast trigger, 82, 100
  - 802.1X unicast trigger, 82, 100
  - FIPS, 580
  - IPsec ACL-based implementation aggregation, 289
  - IPsec ACL-based implementation per-host, 289
  - IPsec ACL-based implementation standard, 289
  - IPsec application-based implementation, 290
  - IPsec encapsulation transport, 287
  - IPsec encapsulation tunnel, 287
  - IPsec IKE negotiation, 288
  - IPsec IKE negotiation (time-based lifetime), 288
  - IPsec IKE negotiation (traffic-based lifetime), 288
  - IPv6 uRPF loose check, 571
  - IPv6 uRPF strict check, 571
  - MAC authentication multi-VLAN, 126
  - PKI offline, 251
  - PKI online, 251
  - port security, 206
  - port security authentication control, 202
  - port security autoLearn MAC learning control, 203
  - port security MAC learning control, 202
  - port security MAC learning control autoLearn, 202
  - port security MAC learning control secure, 202
  - port security macAddressWithRadius authentication, 204
  - port security secure MAC learning control, 203
  - security portal authentication, 136

- security portal authentication (cross-subnet), [137](#)
- security portal authentication (direct), [136](#)
- security portal authentication (re-DHCP), [136](#)
- uRPF loose check, [564](#)
- uRPF strict check, [564](#)
- userLogin 802.1X authentication, [204](#)
- userLoginSecure 802.1X authentication, [204](#)
- userLoginSecureExt 802.1X authentication, [204](#)
- userLoginWithOUI 802.1X authentication, [204](#)

#### MPLS L3VPN

- AAA implementation, [14](#)
- PKI support, [247](#)
- security portal authentication (cross-subnet for MPLS L3VPN), [192](#)

#### multicast

- 802.1X multicast trigger mode, [82](#), [100](#)

#### multichannel protocol (ASPF), [462](#), [465](#)

Multipoint Generic Routing Encapsulation.  
Use [mGRE](#)

## N

#### NAS

- AAA configuration, [18](#)
- AAA device implementation, [12](#)
- AAA HWTACACS implementation, [7](#)
- AAA LDAP implementation, [9](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA NAS-ID profile configuration, [57](#)
- AAA RADIUS implementation, [2](#)
- AAA RADIUS security policy server IP address, [33](#)
- applying interface NAS-ID profile (RADIUS), [156](#)

#### NAS-Port-ID

- specifying format for portal authentication, [154](#)

#### NAT

- IPsec IKE configuration (aggressive mode+NAT traversal), [353](#)

- IPsec IKE keepalive function, [339](#)
- IPsec IKEv2 configuration (NAT traversal), [385](#)
- IPsec IKEv2 keepalive, [372](#)
- mGRE configuration (full-mesh NAT traversal), [612](#)
- mGRE NAT traversal, [592](#)
- session management, [479](#)
- session management configuration, [480](#)

#### NAT-PT

- PKI Keon CA server certificate request, [268](#)

need to know. Use [NTK](#)

#### negotiating

- IPsec IKE negotiation, [331](#)
- IPsec IKE negotiation mode, [288](#)
- IPsec IKEv2 negotiation, [363](#)

#### NETCONF

- enable over SSH, [397](#)
- Secure Telnet client user line configuration, [397](#)
- SSH client user line configuration, [397](#)
- SSH configuration, [453](#)

#### network

- 802.1X access control method, [97](#)
- 802.1X architecture, [79](#)
- 802.1X authentication, [82](#), [83](#)
- 802.1X authentication request attempts max, [98](#)
- 802.1X authentication server timeout timer, [98](#)
- 802.1X authentication trigger, [100](#)
- 802.1X Auth-Fail VLAN, [91](#), [102](#)
- 802.1X authorization state, [96](#)
- 802.1X authorization VLAN assignment configuration, [108](#)
- 802.1X basic configuration, [106](#)
- 802.1X critical VLAN, [91](#), [103](#)
- 802.1X EAD assistant, [104](#)
- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
- 802.1X EAD assistant configuration (DHCP server), [115](#)
- 802.1X EAP over RADIUS, [81](#)

- 802.1X EAP relay authentication, [84](#)
- 802.1X EAP relay enable, [96](#)
- 802.1X EAP relay/termination, [84](#)
- 802.1X EAP termination, [86](#)
- 802.1X EAP termination enable, [96](#)
- 802.1X guest VLAN, [90](#), [102](#)
- 802.1X online user handshake, [99](#)
- 802.1X packet format, [80](#)
- 802.1X periodic online user reauthentication, [101](#)
- 802.1X port users max, [98](#)
- 802.1X related protocols, [80](#)
- 802.1X SmartOn, [105](#)
- 802.1X SmartOn feature configuration, [117](#)
- 802.1X VLAN manipulation, [88](#)
- 802.1X+ACL assignment configuration, [111](#)
- AAA device implementation, [12](#)
- AAA HWTACACS implementation, [7](#)
- AAA HWTACACS scheme, [36](#)
- AAA HWTACACS server PPP user, [75](#)
- AAA HWTACACS server SSH user, [63](#)
- AAA ISP domain accounting method, [52](#)
- AAA ISP domain attribute, [47](#)
- AAA ISP domain authentication method, [49](#)
- AAA ISP domain authorization method, [51](#)
- AAA ISP domain creation, [46](#)
- AAA ISP domain method, [46](#)
- AAA LDAP implementation, [9](#)
- AAA LDAP scheme, [42](#)
- AAA LDAP server SSH user authentication, [65](#)
- AAA LDAP server SSL VPN user authentication+authorization, [70](#)
- AAA local SSH user authentication+authorization, [62](#)
- AAA local user, [20](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA NAS-ID profile configuration, [57](#)
- AAA network access user, [20](#)
- AAA RADIUS implementation, [2](#)
- AAA RADIUS scheme, [25](#)
- AAA RADIUS server SSH user authentication+authorization, [58](#)
- AAA scheme, [19](#)
- applying interface NAS-ID profile, [156](#)
- APR application group configuration, [476](#)
- APR application statistics enable, [476](#)
- APR configuration, [478](#)
- APR PBAR configuration, [475](#)
- ARP active acknowledgement, [551](#)
- ARP attack detection (source MAC-based), [549](#), [550](#)
- ARP attack protection (unresolvable IP attack), [547](#), [548](#)
- ARP attack protection blackhole routing (unresolvable IP attack), [547](#)
- ARP attack protection source suppression (unresolvable IP attack), [547](#)
- ARP detection configuration, [554](#)
- ARP detection packet validity check, [556](#)
- ARP detection restricted forwarding, [556](#), [558](#)
- ARP detection user validity check, [555](#)
- ARP detection user+packet validity check, [557](#)
- ARP filtering, [562](#), [563](#)
- ARP gateway protection, [561](#), [561](#)
- ARP packet source MAC consistency check, [551](#)
- ARP scanning, [560](#)
- ASPF application inspection (FTP), [467](#)
- ASPF application inspection (H.323), [470](#)
- ASPF application inspection (TCP), [468](#)
- ASPF inspection, [463](#)
- ASPF policy, [465](#)
- ASPF policy application (interface), [466](#)
- ASPF policy application (zone pair), [466](#), [471](#)
- attack D&P blacklist configuration, [531](#)
- attack D&P client verification configuration (DNS), [533](#)



- attack D&P client verification configuration (HTTP), [534](#)
- attack D&P client verification configuration (TCP), [532](#)
- attack D&P configuration (interface-based), [528](#)
- attack D&P log aggregation, [520](#)
- attack D&P policy application (device), [519](#)
- authorized ARP (DHCP relay agent), [553](#)
- authorized ARP (DHCP server), [552](#)
- authorized ARP configuration, [551](#)
- connection limit configuration (interface-based), [486](#)
- connection limit policy application, [488](#)
- connection limit policy configuration, [487](#)
- connection limit policy creation, [487](#)
- crypto engine hardware configuration, [577](#)
- FIPS mode entry (automatic reboot), [584](#)
- FIPS mode entry (manual reboot), [585](#)
- FIPS mode exit (automatic reboot), [587](#)
- FIPS mode exit (manual reboot), [587](#)
- fixed ARP configuration, [560](#)
- IP source guard (IPSG) dynamic binding, [537](#)
- IP source guard (IPSG) static binding, [536](#)
- IPsec ACL, [292](#)
- IPsec ACL de-encapsulated packet check, [304](#)
- IPsec ACL-based implementation, [289](#), [292](#)
- IPsec anti-replay, [305](#)
- IPsec anti-replay redundancy, [305](#)
- IPsec application-based implementation, [290](#)
- IPsec crypto engine, [289](#)
- IPsec IKE configuration (aggressive mode+NAT traversal), [353](#)
- IPsec IKE configuration (aggressive mode+RSA signature authentication), [346](#)
- IPsec IKE configuration (main mode/pre-shared key authentication), [342](#)
- IPsec IKE SNMP notification, [341](#)

- IPsec IKEv2 address pool, [372](#)
- IPsec IKEv2 configuration (NAT traversal), [385](#)
- IPsec IKEv2 configuration (pre-shared key authentication), [373](#)
- IPsec IKEv2 configuration (RSA signature authentication), [377](#)
- IPsec implementation, [289](#)
- IPsec IPv6 routing protocol profile (manual), [309](#)
- IPsec IPv6 routing protocols, [309](#)
- IPsec packet DF bit, [307](#)
- IPsec packet logging enable, [307](#)
- IPsec policy (IKE-based), [299](#)
- IPsec policy (IKE-based/direct), [300](#)
- IPsec policy (IKE-based/template), [301](#)
- IPsec policy (manual), [297](#)
- IPsec policy application to interface, [303](#)
- IPsec profile (IKE-based), [311](#)
- IPsec profile application to tunnel interface (IKE-based), [312](#)
- IPsec QoS pre-classify enable, [307](#)
- IPsec RIPng configuration, [324](#)
- IPsec RRI, [290](#)
- IPsec RRI configuration, [308](#), [327](#)
- IPsec SNMP notification, [312](#)
- IPsec source interface policy bind, [306](#)
- IPsec transform set, [295](#)
- IPsec tunnel configuration, [311](#)
- IPsec tunnel establishment, [291](#)
- IPsec tunnel for IPv4 packets (IKE-based), [317](#)
- IPsec tunnel for IPv4 packets (manual), [314](#)
- IPsec tunnel for IPv6 packets (IKE-based), [320](#)
- IPv4 source guard (IPv4SG) configuration, [537](#)
- IPv4 source guard (IPv4SG) dynamic binding configuration, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv4 source guard (IPv4SG) enable on interface, [538](#)

- IPv4 source guard (IPv4SG) static binding configuration, [538](#), [540](#)
- IPv6 source guard (IPv6SG) configuration, [538](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- IPv6 source guard (IPv6SG) enable on interface, [538](#)
- IPv6 source guard (IPv6SG) static binding configuration, [539](#), [543](#)
- IPv6 uRPF application, [574](#)
- IPv6 uRPF check modes, [571](#)
- IPv6 uRPF configuration, [574](#)
- IPv6 uRPF operation, [572](#)
- MAC authentication (local), [127](#)
- MAC authentication (RADIUS-based), [129](#)
- MAC authentication ACL assignment, [121](#), [131](#)
- MAC authentication concurrent port users max, [125](#)
- MAC authentication delay, [125](#)
- MAC authentication domain, [123](#)
- MAC authentication keep-online, [126](#)
- MAC authentication methods, [120](#)
- MAC authentication multi-VLAN mode, [126](#)
- MAC authentication timer, [124](#)
- MAC authentication user account format, [124](#)
- MAC authentication VLAN assignment, [121](#)
- mGRE configuration (full-mesh NAT traversal), [612](#)
- mGRE configuration (full-mesh), [594](#), [601](#)
- mGRE configuration (NHS-NHC), [598](#), [607](#)
- mGRE NAT traversal, [592](#)
- NETCONF-over-SSH client user line, [397](#)
- NETCONF-over-SSH configuration, [453](#)
- NETCONF-over-SSH enable, [397](#)
- password control parameters (global), [229](#)
- password control parameters (local user), [231](#)
- password control parameters (super), [231](#)

- password control parameters (user group), [230](#)
- peer public key entry, [240](#)
- periodic MAC reauthentication, [121](#)
- PKI applications, [247](#)
- PKI architecture, [246](#)
- PKI CA policy, [246](#)
- PKI CA storage path, [256](#)
- PKI certificate import/export, [275](#)
- PKI certificate request, [251](#)
- PKI certificate-based access control policy, [274](#)
- PKI CRL, [245](#)
- PKI digital certificate, [245](#)
- PKI domain configuration, [249](#)
- PKI entity configuration, [248](#)
- PKI MPLS L3VPN support, [247](#)
- PKI OpenCA server certificate request, [265](#)
- PKI operation, [246](#)
- PKI RSA Keon CA server certificate request, [259](#)
- PKI RSA Keon CA server certificate request (NAT-PT network), [268](#)
- PKI Windows 2003 CA server certificate request, [261](#)
- PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)
- port security authorization-fail-offline, [212](#)
- port security client
  - macAddressElseUserLoginSecure, [218](#)
  - port security client userLoginWithOUI, [215](#)
- port security features, [202](#), [208](#)
- port security intrusion protection, [208](#)
- port security MAC address autoLearn, [213](#)
- port security MAC address learning control, [203](#)
- port security mode, [202](#), [206](#)
- port security NAS-ID profile, [212](#)
- port security NTK, [208](#)
- port security secure MAC address, [209](#)
- port security secure MAC address port limit, [206](#)
- public key import from file, [242](#)
- Secure Telnet client user line, [397](#)



- security portal authentication AAA server, 135
- security portal authentication client, 135
- security portal authentication domain, 146
- security portal authentication system components, 134
- security portal preauthentication domain, 147
- session management aging time (application layer protocol), 481
- session management aging time (protocol state), 480
- session management functions, 479
- session management logging, 482
- session management persistent session, 482
- session management statistics collection, 482
- SSH client host public key configuration, 398
- SSH management parameters, 400
- SSH SCP client device, 411
- SSH SCP configuration, 444
- SSH SCP configuration (Suite B), 446
- SSH SCP file transfer+password authentication, 444
- SSH SCP server connection establishment, 412
- SSH SCP server connection establishment based on Suite B, 415
- SSH SCP server enable, 397
- SSH Secure Telnet client device, 402
- SSH Secure Telnet client password authentication, 425
- SSH Secure Telnet client publickey authentication, 429
- SSH Secure Telnet configuration, 417
- SSH Secure Telnet configuration (128-bit Suite B), 431
- SSH Secure Telnet packet source IP address, 402
- SSH Secure Telnet server connection establishment, 403
- SSH Secure Telnet server connection establishment based on Suite B, 406

- SSH Secure Telnet server enable, 396
- SSH Secure Telnet server password authentication, 417
- SSH Secure Telnet server publickey authentication, 420
- SSH server configuration, 395
- SSH SFTP client device, 406
- SSH SFTP client publickey authentication, 437
- SSH SFTP configuration, 435
- SSH SFTP configuration (192-bit Suite B), 440
- SSH SFTP directories, 410
- SSH SFTP files, 410
- SSH SFTP packet source IP address, 407
- SSH SFTP server connection establishment, 407
- SSH SFTP server connection establishment based on Suite B, 409
- SSH SFTP server connection termination, 411
- SSH SFTP server enable, 396
- SSH SFTP server password authentication, 435
- SSH user configuration, 399
- SSH2 algorithms, 415
- SSH2 algorithms (encryption ), 416
- SSH2 algorithms (key exchange), 415
- SSH2 algorithms (MAC), 416
- SSH2 algorithms (public key), 416
- SSL client policy configuration, 458
- SSL protocol stack, 455
- SSL server policy configuration, 456, 459
- uRPF application, 568
- uRPF check modes, 564
- uRPF configuration, 568
- uRPF operation, 565

network management

- 802.1X authentication configuration, 106
- 802.1X configuration, 88, 95
- 802.1X guest VLAN assignment configuration, 108
- 802.1X overview, 79
- AAA configuration, 1, 18, 58

- AAA HWTACACS/RADIUS differences, [7](#)
- APR configuration, [474](#)
- ARP attack protection configuration, [546](#)
- ASPF configuration, [462](#), [465](#), [467](#)
- attack D&P configuration, [503](#), [511](#), [528](#)
- connection limit configuration, [486](#), [489](#)
- crypto engine configuration, [577](#)
- FIPS configuration, [579](#), [584](#)
- IP source guard (IPSG) configuration, [536](#), [537](#), [540](#)
- IPsec configuration, [286](#), [314](#)
- IPsec IKE configuration, [331](#), [333](#), [342](#)
- IPsec IKEv2 configuration, [363](#), [364](#), [373](#)
- IPv6 uRPF configuration, [571](#), [575](#)
- MAC authentication, [123](#), [127](#)
- MAC authentication configuration, [120](#)
- object group configuration, [493](#)
- object policy configuration, [495](#), [499](#)
- password control configuration, [225](#), [228](#), [232](#)
- PKI configuration, [245](#), [248](#), [259](#)
- port security configuration, [202](#), [205](#), [213](#)
- public key management, [236](#), [240](#)
- security portal authentication, [139](#)
- security portal authentication configuration, [134](#), [134](#)
- session management, [479](#)
- session management configuration, [480](#)
- SSH configuration, [392](#)
- SSL configuration, [455](#), [456](#)
- SSL services, [455](#)
- uRPF configuration, [564](#), [569](#)
- user profile configuration, [223](#)
- NHC
  - IPsec for mGRE tunnel configuration, [593](#)
  - mGRE operation scheme, [589](#)
  - mGRE routing configuration, [593](#)
  - mGRE tunnel configuration, [592](#)
- NHRP
  - mGRE configuration, [589](#), [592](#), [594](#)
  - mGRE configuration (full-mesh NAT traversal), [612](#)
  - mGRE configuration (full-mesh), [594](#), [601](#)
  - mGRE configuration (NHS-NHC), [598](#), [607](#)
  - mGRE tunnel configuration, [592](#)
- NHS
  - mGRE operation scheme, [589](#)
- NHS-NHC
  - mGRE configuration, [598](#), [607](#)
  - mGRE network type, [590](#)
- no
  - AAA no accounting method, [13](#)
  - AAA no authentication, [13](#)
  - AAA no authorization, [13](#)
- notifying
  - AAA RADIUS SNMP notification, [35](#)
  - IPsec IKE SNMP notification, [341](#)
  - IPsec SNMP notification, [312](#)
- NTK
  - ntkonly mode, [208](#)
  - ntk-withbroadcasts mode, [208](#)
  - ntk-withmulticasts mode, [208](#)
  - port security feature, [202](#)
- numbering
  - IPsec IKE SA max, [341](#)
  - object policy rule numbering, [495](#)
- O**
  - object group
    - configuration, [493](#)
    - display, [494](#)
    - IPv4 address object group, [493](#)
    - IPv4 address object group configuration, [493](#)
    - IPv6 address object group, [493](#)
    - IPv6 address object group configuration, [493](#)
    - port object group, [493](#)
    - port object group configuration, [494](#)
    - service object group, [493](#)
    - service object group configuration, [494](#)

## object policy

- configuration, [495](#), [499](#)
- creation, [496](#)
- display, [499](#)
- IPv4 rule configuration, [496](#)
- IPv4 zone pair application, [498](#)
- IPv6 rule configuration, [496](#)
- IPv6 zone pair application, [498](#)
- rule, [495](#)
- rule configuration, [496](#)
- rule description, [495](#)
- rule match order, [495](#)
- rule match order change, [498](#)
- rule matching acceleration, [498](#)
- rule numbering, [495](#)
- zone pair application, [498](#)

## obtaining

- PKI certificate, [253](#)

## offline

- MAC authentication offline detect, [124](#)
- PKI offline mode, [251](#)
- port security authorization-fail-offline feature, [212](#)

## online

- 802.1X online user handshake, [99](#)
- 802.1X periodic online user reauthentication, [101](#)
- MAC authentication keep-online, [126](#)
- PKI online mode, [251](#)
- security portal authentication user online detection, [149](#)

## OpenCA

- PKI CA server certificate request, [265](#)

## operation procedure

- mGRE, [589](#)

## OSPF

- mGRE routing configuration, [593](#)

## overview

- mGRE, [589](#)

## P

### packet

- 802.1X EAP format, [80](#)
- 802.1X EAPOL format, [81](#)
- 802.1X format, [80](#)
- AAA HWTACACS outgoing packet source IP address, [39](#)
- AAA HWTACACS packet exchange process, [7](#)
- AAA RADIUS outgoing packet source IP address, [30](#)
- AAA RADIUS packet exchange process, [3](#)
- AAA RADIUS packet format, [3](#)
- ARP active acknowledgement, [551](#)
- ARP attack protection (unresolvable IP attack), [547](#), [548](#)
- ARP attack protection blackhole routing (unresolvable IP attack), [547](#)
- ARP attack protection source suppression (unresolvable IP attack), [547](#)
- ARP detection packet validity check, [556](#)
- ARP detection user+packet validity check, [557](#)
- ARP filtering, [562](#), [563](#)
- ARP packet source MAC consistency check, [551](#)
- attack D&P blacklist, [506](#), [522](#)
- attack D&P TCP fragment attack prevention, [520](#)
- IPsec ACL de-encapsulated packet check, [304](#)
- IPsec anti-replay, [305](#)
- IPsec crypto engine, [289](#)
- IPsec implementation, [289](#)
- IPsec packet DF bit, [307](#)
- IPsec packet logging enable, [307](#)
- IPsec QoS pre-classify enable, [307](#)
- IPv6 uRPF configuration, [571](#), [574](#), [575](#)
- object group configuration, [493](#)
- security portal authentication BAS-IP for unsolicited portal packets, [153](#)
- uRPF configuration, [564](#), [568](#), [569](#)

### packet filtering

- ASPF application inspection (FTP), [467](#)

- ASPF application inspection (H.323), 470
- ASPF application inspection (TCP), 468
- ASPF configuration, 462, 465, 467
- IP source guard (IPSG)
  - configuration, 536, 537, 540
- IPv4 source guard (IPv4SG) dynamic binding
  - configuration, 541
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, 542
- IPv4 source guard (IPv4SG) static binding
  - configuration, 540
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, 544
- IPv6 source guard (IPv6SG) static binding
  - configuration, 543
- parameter
  - AAA RADIUS accounting server
    - parameters, 27
  - AAA RADIUS class attribute as CAR
    - parameter, 33
  - configuring SSH management
    - parameters, 400
  - password control parameters (global), 229
  - password control parameters (local user), 231
  - password control parameters (super), 231
  - password control parameters (user group), 230
- password
  - SSH password authentication, 393
  - SSH password-publickey authentication, 393
  - SSH SCP file transfer+password authentication, 444
  - SSH Secure Telnet client password authentication, 425
  - SSH Secure Telnet server password authentication, 417
  - SSH SFTP server password authentication, 435
- password control
  - configuration, 225, 228, 232
- display, 232
- enable, 228
- event logging, 227
- expired password login, 226
- FIPS compliance, 228
- maintain, 232
- max user account idle time, 227
- parameters (global), 229
- parameters (local user), 231
- parameters (super), 231
- parameters (user group), 230
- password complexity checking, 225
- password composition checking, 225
- password expiration, 226, 226
- password history, 226
- password minimum length, 225
- password not displayed, 227
- password setting, 225
- password updating, 226, 226
- user first login, 227
- user login attempt limit, 227
- user login control, 227
- path
  - troubleshooting PKI storage path set failure, 285
- PBAR
  - APR configuration, 478
  - APR configuration (port-based), 474
  - configuration, 475
- peer
  - IPsec implementation, 289
  - IPsec SA, 288
  - IPsec source interface policy bind, 306
  - peer public key entry, 239
  - peer public key import from file, 239
  - PKI digital certificate, 245
  - public key peer configuration, 239
- per-destination connection limit rule, 487
- Perfect Forward Secrecy. See PFS
- periodic MAC reauthentication, 121

per-service connection limit rule, [487](#)

persistent session, [482](#)

per-source connection limit rule, [487](#)

PFS (IKE), [333](#)

PKI

applications, [247](#)

architecture, [246](#)

CA digital certificate, [245](#)

CA policy, [246](#)

CA storage path, [256](#)

certificate export, [256](#)

certificate import/export, [275](#)

certificate obtain, [253](#)

certificate removal, [257](#)

certificate request, [251](#)

certificate request (automatic), [252](#)

certificate request (manual), [252](#)

certificate request abort, [253](#)

certificate verification, [254](#)

certificate verification (CRL checking), [254](#)

certificate verification (w/o CRL checking), [255](#)

certificate-based access control

policy, [257](#), [274](#)

configuration, [245](#), [248](#), [259](#)

CRL, [245](#)

display, [258](#)

domain configuration, [249](#)

entity configuration, [248](#)

FIPS compliance, [248](#)

local digital certificate, [245](#)

MPLS L3VPN support, [247](#)

OpenCA server certificate request, [265](#)

operation, [246](#)

peer digital certificate, [245](#)

public key management, [236](#), [240](#)

RA digital certificate, [245](#)

RSA Keon CA server certificate request, [259](#)

RSA Keon CA server certificate request  
(NAT-PT network), [268](#)

terminology, [245](#)

troubleshoot CA certificate import failure, [283](#)

troubleshoot CA certificate obtain failure, [281](#)

troubleshoot certificate export failure, [284](#)

troubleshoot configuration, [281](#)

troubleshoot CRL obtain failure, [283](#)

troubleshoot local certificate import failure, [284](#)

troubleshoot local certificate obtain failure, [281](#)

troubleshoot local certificate request failure, [282](#)

troubleshoot storage path set failure, [285](#)

Windows 2003 CA server certificate request  
configuration, [261](#)

Windows 2003 CA server IKE negotiation+RSA  
digital signature, [271](#)

policy

AAA ITA policy configuration, [56](#)

AAA RADIUS security policy server IP  
address, [33](#)

ASPF, [465](#)

ASPF policy application (interface), [466](#)

ASPF policy application (zone pair), [466](#), [471](#)

attack D&P defense policy, [511](#)

attack D&P defense policy (flood), [513](#)

attack D&P defense policy (scanning), [513](#)

attack D&P defense policy (single-packet), [511](#)

connection limit policy application, [488](#)

connection limit policy configuration, [487](#)

connection limit policy creation, [487](#)

IPsec (manual), [297](#)

IPsec application to interface, [303](#)

IPsec IKEv2 configuration, [368](#)

IPsec policy (IKE-based), [299](#)

IPsec policy (IKE-based/direct), [300](#)

IPsec policy (IKE-based/template), [301](#)

IPsec QoS pre-classify enable, [307](#)

IPsec source interface policy bind, [306](#)

IPsec transform set, [295](#)

MAC authentication user account policies, [120](#)

object group configuration, [493](#)

- password control configuration, [225](#), [228](#), [232](#)
- PKI CA policy, [246](#)
- PKI certificate-based access control policy, [257](#)
- security portal authentication extended functions, [134](#)
- security portal authentication policy server, [135](#)
- SSL client policy configuration, [458](#)
- SSL server policy configuration, [456](#), [459](#)

## port

- 802.1X Auth-Fail VLAN, [102](#)
- 802.1X critical VLAN, [103](#)
- 802.1X guest VLAN, [102](#)
- applying interface NAS-ID profile, [156](#)
- APR configuration, [474](#), [478](#)
- APR PBAR configuration, [475](#)
- APR PBAR mapping, [474](#)
- MAC authentication, [123](#), [127](#)
- MAC authentication (local), [127](#)
- MAC authentication (RADIUS-based), [129](#)
- MAC authentication concurrent port users max, [125](#)
- MAC authentication configuration, [120](#)
- MAC authentication delay, [125](#)
- MAC authentication multi-VLAN mode, [126](#)
- object group, [493](#)
- object group configuration, [494](#)
- security. See [port security](#)
- security portal authentication, [139](#)
- security portal authentication configuration, [134](#), [157](#)

## port security

- 802.1X access control method, [97](#)
- 802.1X authentication, [204](#)
- 802.1X authentication configuration, [106](#)
- 802.1X authorization state, [96](#)
- 802.1X authorization status, [79](#)

- 802.1X authorization VLAN assignment configuration, [108](#)
- 802.1X basic configuration, [106](#)
- 802.1X configuration, [88](#), [95](#)
- 802.1X controlled/uncontrolled port, [79](#)
- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
- 802.1X EAD assistant configuration (DHCP server), [115](#)
- 802.1X guest VLAN assignment configuration, [108](#)
- 802.1X mandatory port authentication domain, [100](#)
- 802.1X overview, [79](#)
- 802.1X port users max, [98](#)
- 802.1X SmartOn feature configuration, [117](#)
- 802.1X+ACL assignment configuration, [111](#)
- authentication modes, [202](#)
- authorization-fail-offline, [212](#)
- client macAddressElseUserLoginSecure, [218](#)
- client userLoginWithOUI, [215](#)
- configuration, [202](#), [205](#), [213](#)
- display, [213](#)
- enable, [205](#)
- feature configuration, [208](#)
- features, [202](#)
- intrusion protection, [208](#)
- intrusion protection feature, [202](#)
- MAC address autoLearn, [213](#)
- MAC address learning control, [203](#)
- MAC authentication, [204](#)
- MAC move enable, [211](#)
- MAC+802.1X authentication, [204](#)
- mode set, [206](#)
- NAS-ID profile application, [212](#)
- NTK configuration, [208](#)
- NTK feature, [202](#)
- secure MAC address, [209](#)
- secure MAC address port limit, [206](#)

- server authorization information, 211
- troubleshoot, 222
- troubleshoot mode cannot be set, 222
- troubleshoot secure MAC addresses, 222

portal

- command and hardware compatibility, 139
- user profile configuration, 223

portal authentication

- AAA server, 135
- access device, 135
- authentication destination subnet, 145
- authentication modes, 136
- authentication process, 137
- authentication server, 135
- authentication source subnet, 144
- BAS-IP, 153
- client, 135
- configuration, 134, 139, 157
- configuration restrictions, 142
- configuring preauthentication IP address pool, 148
- cross-subnet authentication, 170
- cross-subnet for MPLS L3VPN, 192
- detection features, 149
- direct authentication configuration, 157
- direct authentication configuration with preauthentication domain, 194
- direct/cross-subnet authentication process (with CHAP/PAP authentication), 137
- displaying, 156
- domain specification, 146, 147
- enabling, 141
- enabling strict-checking mode, 148
- extended cross-subnet authentication configuration, 180
- extended direct authentication configuration, 173
- extended functions, 134
- extended re-DHCP, 176
- fail-permit configuration, 153
- maintaining, 156
- max number users, 145
- outgoing packets filtering, 149
- portal-free rule, 143
- re-DHCP, 167
- re-DHCP with preauthentication domain, 196
- roaming enable, 154
- security policy server, 135
- server configuration, 140
- server detection, 150
- server detection+user synchronization configuration, 184
- specifying NAS-Port-ID attribute format, 154
- system component interaction, 136
- system components, 134
- troubleshooting, 199
- troubleshooting cannot log out users (access device), 199
- troubleshooting cannot log out users (RADIUS server), 200
- troubleshooting no page pushed for users, 199
- troubleshooting users logged out still exist on server, 200
- types, 134
- user access control, 143
- user logout, 155
- user online detection, 149
- user synchronization configuration, 152
- users cannot log in (re-DHCP), 200
- Web redirect configuration, 155
- Web server, 135
- Web server configuration, 141
- Web server detection configuration, 151
- Web server reference, 142

port-based application recognition. See **PBAR**

power-up self-test, 583

PPP

- AAA HWTACACS server PPP user, 75



## PPPoE

- user profile configuration, [223](#)

## preventing

- attack detection and prevention. See [attack D&P](#)

## priority

- AAA RADIUS packet DSCP priority change, [55](#)

## procedure

- applying ASPF policy (interface), [466](#)
- applying ASPF policy (zone pair), [466](#)
- applying connection limit policy, [488](#)
- applying interface NAS-ID profile, [156](#)
- applying IPsec policy to interface, [303](#)
- applying IPsec profile to tunnel interface (IKE-based), [312](#)
- applying IPv4 object policy to zone pair, [498](#)
- applying IPv6 object policy to zone pair, [498](#)
- applying port security NAS-ID profile, [212](#)
- authenticating with 802.1X EAP relay, [84](#)
- authenticating with 802.1X EAP termination, [86](#)
- binding IPsec source interface to policy, [306](#)
- changing AAA RADIUS packet DSCP priority, [55](#)
- changing IPv4 object policy rule match order, [498](#)
- changing IPv6 object policy rule match order, [498](#)
- configuring 802.1X, [95](#)
- configuring 802.1X authentication trigger, [100](#)
- configuring 802.1X Auth-Fail VLAN, [102](#)
- configuring 802.1X authorization VLAN assignment, [108](#)
- configuring 802.1X basics, [106](#)
- configuring 802.1X critical VLAN, [103](#)
- configuring 802.1X EAD assistant, [104](#)
- configuring 802.1X EAD assistant (DHCP relay agent), [112](#)

- configuring 802.1X EAD assistant (DHCP server), [115](#)

- configuring 802.1X guest VLAN, [102](#)

- configuring 802.1X guest VLAN assignment, [108](#)

- configuring 802.1X online user handshake, [99](#)

- configuring 802.1X SmartOn, [105](#), [117](#)

- configuring 802.1X+ACL assignment, [111](#)

- configuring AAA, [18](#)

- configuring AAA HWTACACS schemes, [36](#)

- configuring AAA HWTACACS server PPP user, [75](#)

- configuring AAA HWTACACS server SSH user, [63](#)

- configuring AAA ISP domain accounting method, [52](#)

- configuring AAA ISP domain attribute, [47](#)

- configuring AAA ISP domain authentication method, [49](#)

- configuring AAA ISP domain authorization method, [51](#)

- configuring AAA ISP domain method, [46](#)

- configuring AAA LDAP administrator attributes, [43](#)

- configuring AAA LDAP attribute map, [44](#)

- configuring AAA LDAP scheme, [42](#)

- configuring AAA LDAP server IP address, [42](#)

- configuring AAA LDAP server SSH user authentication, [65](#)

- configuring AAA LDAP server SSL VPN user authentication+authorization, [70](#)

- configuring AAA LDAP user attributes, [43](#)

- configuring AAA local SSH user authentication+authorization, [62](#)

- configuring AAA local user, [20](#)

- configuring AAA local user attributes, [21](#)

- configuring AAA NAS-ID profile, [57](#)

- configuring AAA RADIUS Acct-Session-Id format, [57](#)

- configuring AAA RADIUS DAE server, [55](#)



configuring AAA RADIUS Login-Service attribute check method, [34](#)  
configuring AAA RADIUS scheme, [25](#)  
configuring AAA RADIUS security policy server IP address, [33](#)  
configuring AAA RADIUS server SSH user authentication+authorization, [58](#)  
configuring AAA RADIUS server status detection test profile, [25](#)  
configuring AAA scheme, [19](#)  
configuring AAA user group attributes, [23](#)  
configuring and applying AAA ITA policy, [56](#)  
configuring APR, [478](#)  
configuring APR application groups, [476](#)  
configuring APR PBAR, [475](#)  
configuring ARP active acknowledgement, [551](#)  
configuring ARP attack detection (source MAC-based), [549](#), [550](#)  
configuring ARP attack protection (unresolvable IP attack), [547](#), [548](#)  
configuring ARP attack protection blackhole routing (unresolvable IP attack), [547](#)  
configuring ARP attack protection source suppression (unresolvable IP attack), [547](#)  
configuring ARP detection, [554](#)  
configuring ARP detection packet validity check, [556](#)  
configuring ARP detection restricted forwarding, [556](#), [558](#)  
configuring ARP detection user validity check, [555](#)  
configuring ARP detection user+packet validity check, [557](#)  
configuring ARP filtering, [562](#), [563](#)  
configuring ARP gateway protection, [561](#), [561](#)  
configuring ARP packet source MAC consistency check, [551](#)  
configuring ARP scanning, [560](#)  
configuring ASPF, [465](#)

configuring ASPF application inspection (FTP), [467](#)  
configuring ASPF application inspection (H.323), [470](#)  
configuring ASPF application inspection (TCP), [468](#)  
configuring ASPF policy, [465](#)  
configuring ASPF policy application (zone pair), [471](#)  
configuring attack D&P, [511](#)  
configuring attack D&P (interface-based), [528](#)  
configuring attack D&P blacklist, [522](#), [531](#)  
configuring attack D&P client verification (DNS), [521](#), [533](#)  
configuring attack D&P client verification (HTTP), [522](#), [534](#)  
configuring attack D&P client verification (TCP), [520](#), [532](#)  
configuring attack D&P defense policy, [511](#)  
configuring attack D&P defense policy (ACK flood), [514](#)  
configuring attack D&P defense policy (DNS flood), [517](#)  
configuring attack D&P defense policy (FIN flood), [515](#)  
configuring attack D&P defense policy (flood), [513](#)  
configuring attack D&P defense policy (HTTP flood), [518](#)  
configuring attack D&P defense policy (ICMP flood), [516](#)  
configuring attack D&P defense policy (ICMPv6 flood), [516](#)  
configuring attack D&P defense policy (RST flood), [515](#)  
configuring attack D&P defense policy (scanning), [513](#)  
configuring attack D&P defense policy (single-packet), [511](#)  
configuring attack D&P defense policy (SYN flood), [514](#)

- configuring attack D&P defense policy (SYN-ACK flood), [514](#)
- configuring attack D&P defense policy (UDP flood), [517](#)
- configuring attack D&P detection exemption, [518](#)
- configuring attack D&P policy application (device), [519](#)
- configuring attack D&P policy application (interface), [519](#)
- configuring attack D&P TCP fragment attack prevention, [520](#)
- configuring authorized ARP configuration, [551](#)
- configuring authorized ARP configuration (DHCP relay agent), [553](#)
- configuring authorized ARP configuration (DHCP server), [552](#)
- configuring connection limit, [489](#)
- configuring connection limit (interface-based), [486](#)
- configuring connection limit policy, [487](#)
- configuring crypto engine (hardware), [577](#)
- configuring FIPS mode, [580](#)
- configuring FIPS mode entry (automatic reboot), [584](#)
- configuring FIPS mode entry (manual reboot), [585](#)
- configuring FIPS mode exit (automatic reboot), [587](#)
- configuring FIPS mode exit (manual reboot), [587](#)
- configuring fixed ARP, [560](#)
- configuring IP source guard (IPSG), [537](#)
- configuring IPsec ACL, [292](#)
- configuring IPsec ACL anti-replay, [305](#)
- configuring IPsec anti-replay redundancy, [305](#)
- configuring IPsec for IPv6 routing protocols, [309](#)
- configuring IPsec for mGRE tunnel, [593](#)
- configuring IPsec IKE, [333](#)

- configuring IPsec IKE (aggressive mode+NAT traversal), [353](#)
- configuring IPsec IKE (aggressive mode+RSA signature authentication), [346](#)
- configuring IPsec IKE (main mode/pre-shared key authentication), [342](#)
- configuring IPsec IKE DPD, [340](#)
- configuring IPsec IKE global identity information, [338](#)
- configuring IPsec IKE keepalive function, [339](#)
- configuring IPsec IKE keychain, [337](#)
- configuring IPsec IKE NAT keepalive function, [339](#)
- configuring IPsec IKE profile, [334](#)
- configuring IPsec IKE proposal, [336](#)
- configuring IPsec IKE SA max, [341](#)
- configuring IPsec IKE SNMP notification, [341](#)
- configuring IPsec IKEv2, [364](#)
- configuring IPsec IKEv2 (NAT traversal), [385](#)
- configuring IPsec IKEv2 (pre-shared key authentication), [373](#)
- configuring IPsec IKEv2 (RSA signature authentication), [377](#)
- configuring IPsec IKEv2 address pool, [372](#)
- configuring IPsec IKEv2 DPD, [371](#)
- configuring IPsec IKEv2 global parameters, [371](#)
- configuring IPsec IKEv2 keychain, [370](#)
- configuring IPsec IKEv2 NAT keepalive, [372](#)
- configuring IPsec IKEv2 policy, [368](#)
- configuring IPsec IKEv2 profile, [365](#)
- configuring IPsec IKEv2 proposal, [369](#)
- configuring IPsec IPv6 routing protocol profile (manual), [309](#)
- configuring IPsec packet DF bit, [307](#)
- configuring IPsec policy (IKE-based), [299](#)
- configuring IPsec policy (IKE-based/direct), [300](#)
- configuring IPsec policy (IKE-based/template), [301](#)
- configuring IPsec policy (manual), [297](#)
- configuring IPsec profile (IKE-based), [311](#)

- configuring IPsec RIPng, [324](#)
- configuring IPsec RRI, [308](#), [327](#)
- configuring IPsec SNMP notification, [312](#)
- configuring IPsec transform set, [295](#)
- configuring IPsec tunnel, [311](#)
- configuring IPsec tunnel for IPv4 packets (IKE-based), [317](#)
- configuring IPsec tunnel for IPv4 packets (manual), [314](#)
- configuring IPsec tunnel for IPv6 packets (IKE-based), [320](#)
- configuring IPv4 address object group, [493](#)
- configuring IPv4 object policy rule, [496](#)
- configuring IPv4 source guard (IPv4SG), [537](#)
- configuring IPv4 source guard (IPv4SG) dynamic binding, [541](#)
- configuring IPv4 source guard (IPv4SG) dynamic binding+DHCP relay, [542](#)
- configuring IPv4 source guard (IPv4SG) static binding, [538](#), [540](#)
- configuring IPv6 address object group, [493](#)
- configuring IPv6 object policy rule, [496](#)
- configuring IPv6 source guard (IPv6SG), [538](#)
- configuring IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping, [544](#)
- configuring IPv6 source guard (IPv6SG) static binding, [539](#), [543](#)
- configuring IPv6 uRPF, [574](#), [575](#)
- configuring MAC authentication, [123](#)
- configuring MAC authentication (local), [127](#)
- configuring MAC authentication (RADIUS-based), [129](#)
- configuring MAC authentication ACL assignment, [131](#)
- configuring MAC authentication delay, [125](#)
- configuring MAC authentication keep-online, [126](#)
- configuring MAC authentication multi-VLAN mode, [126](#)
- configuring MAC authentication timer, [124](#)

- configuring MAC authentication user account format, [124](#)
- configuring mGRE, [592](#)
- configuring mGRE (full-mesh NAT traversal), [612](#)
- configuring mGRE (full-mesh), [594](#), [601](#)
- configuring mGRE (NHS-NHC), [598](#), [607](#)
- configuring mGRE routing, [593](#)
- configuring mGRE tunnel, [592](#)
- configuring NETCONF-over-SSH client user line, [397](#)
- configuring object policy, [499](#)
- configuring password control, [228](#)
- configuring PKI, [248](#)
- configuring PKI certificate import/export, [275](#)
- configuring PKI certificate request (automatic), [252](#)
- configuring PKI certificate request (manual), [252](#)
- configuring PKI certificate request abort, [253](#)
- configuring PKI certificate-based access control policy, [257](#), [274](#)
- configuring PKI domain, [249](#)
- configuring PKI entity, [248](#)
- configuring PKI Keon CA server certificate request (NAT-PT network), [268](#)
- configuring PKI OpenCA server certificate request, [265](#)
- configuring PKI RSA Keon CA server certificate request, [259](#)
- configuring PKI Windows 2003 CA server certificate request, [261](#)
- configuring PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)
- configuring port object group, [494](#)
- configuring port security, [205](#)
- configuring port security client macAddressElseUserLoginSecure, [218](#)
- configuring port security client userLoginWithOUI, [215](#)
- configuring port security features, [208](#)
- configuring port security intrusion protection, [208](#)

configuring port security MAC address autoLearn, [213](#)  
configuring port security NTK, [208](#)  
configuring port security secure MAC addresses, [209](#)  
configuring preauthentication IP address pool for portal user, [148](#)  
configuring public peer key, [239](#)  
configuring Secure Telnet client user line, [397](#)  
configuring security password control, [232](#)  
configuring security portal authentication, [139](#), [157](#)  
configuring security portal authentication (cross-subnet for MPLS L3VPN), [192](#)  
configuring security portal authentication cross-subnet, [170](#)  
configuring security portal authentication destination subnet, [145](#)  
configuring security portal authentication detection features, [149](#)  
configuring security portal authentication direct, [157](#)  
configuring security portal authentication direct with preauthentication domain, [194](#)  
configuring security portal authentication extended cross-subnet, [180](#)  
configuring security portal authentication extended direct, [173](#)  
configuring security portal authentication extended re-DHCP, [176](#)  
configuring security portal authentication fail-permit, [153](#)  
configuring security portal authentication portal-free rule, [143](#)  
configuring security portal authentication re-DHCP, [167](#)  
configuring security portal authentication re-DHCP with preauthentication domain, [196](#)  
configuring security portal authentication server, [140](#)

configuring security portal authentication server BAS-IP, [153](#)  
configuring security portal authentication server detection, [150](#)  
configuring security portal authentication server detection+user synchronization, [184](#)  
configuring security portal authentication source subnet, [144](#)  
configuring security portal authentication user online detection, [149](#)  
configuring security portal authentication user synchronization, [152](#)  
configuring security portal authentication Web server, [141](#)  
configuring security portal authentication Web server detection, [151](#)  
configuring service object group, [494](#)  
configuring session management, [480](#)  
configuring session management logging, [482](#)  
configuring SSH client host public key, [398](#)  
configuring SSH device as Secure Telnet client, [402](#)  
configuring SSH device as server, [395](#)  
configuring SSH device as SFTP client, [406](#)  
configuring SSH management parameters, [400](#)  
configuring SSH SCP client device, [411](#)  
configuring SSH Secure Telnet client password authentication, [425](#)  
configuring SSH Secure Telnet client publickey authentication, [429](#)  
configuring SSH Secure Telnet server password authentication, [417](#)  
configuring SSH Secure Telnet server publickey authentication, [420](#)  
configuring SSH SFTP client publickey authentication, [437](#)  
configuring SSH SFTP server password authentication, [435](#)  
configuring SSH user, [399](#)  
configuring SSH2 algorithms (encryption ), [416](#)

- configuring SSH2 algorithms (key exchange), [415](#)
- configuring SSH2 algorithms (MAC), [416](#)
- configuring SSH2 algorithms (public key), [416](#)
- configuring SSL, [456](#)
- configuring SSL client policy, [458](#)
- configuring SSL server policy, [456](#), [459](#)
- configuring uRPF, [568](#), [569](#)
- configuring user profile, [223](#), [224](#)
- configuring Web redirect, [155](#)
- controlling security portal authentication user access, [143](#)
- creating AAA HWTACACS scheme, [36](#)
- creating AAA ISP domain, [46](#)
- creating AAA LDAP scheme, [45](#)
- creating AAA LDAP server, [42](#)
- creating AAA RADIUS scheme, [26](#)
- creating attack D&P defense policy, [511](#)
- creating connection limit policy, [487](#)
- creating IPv4 object policy, [496](#)
- creating IPv6 object policy, [496](#)
- creating local key pair, [236](#)
- destroying local key pair, [238](#)
- disabling attack D&P log aggregation, [520](#)
- displaying 802.1X, [106](#)
- displaying AAA, [58](#)
- displaying AAA HWTACACS, [41](#)
- displaying AAA LDAP, [46](#)
- displaying AAA local users/user groups, [24](#)
- displaying AAA RADIUS, [35](#)
- displaying APR, [477](#)
- displaying ARP attack detection (source MAC-based), [549](#)
- displaying ARP attack protection (unresolvable IP attack), [547](#)
- displaying ARP detection, [557](#)
- displaying ASPF, [467](#)
- displaying attack D&P, [523](#)
- displaying connection limit, [488](#)

- displaying crypto engine, [578](#)
- displaying FIPS, [584](#)
- displaying host public key, [238](#)
- displaying IP source guard (IPSG), [539](#)
- displaying IPsec, [313](#)
- displaying IPsec IKE, [342](#)
- displaying IPsec IKEv2, [372](#)
- displaying IPv4 source guard (IPv4SG), [539](#)
- displaying IPv6 source guard (IPv6SG), [539](#)
- displaying IPv6 uRPF, [575](#)
- displaying MAC authentication, [127](#)
- displaying mGRE, [594](#)
- displaying object group, [494](#)
- displaying object policy, [499](#)
- displaying port security, [213](#)
- displaying public key, [240](#)
- displaying security password control, [232](#)
- displaying security PKI, [258](#)
- displaying security portal authentication, [156](#)
- displaying security SSL, [459](#)
- displaying session management, [483](#)
- displaying SSH, [417](#)
- displaying SSH SFTP help information, [411](#)
- displaying uRPF, [569](#)
- displaying user profile, [224](#)
- distributing local host public key, [237](#)
- enabling 802.1X, [95](#)
- enabling 802.1X EAP relay, [96](#)
- enabling 802.1X EAP termination, [96](#)
- enabling 802.1X periodic online user reauthentication, [101](#)
- enabling AAA RADIUS accounting-on, [32](#)
- enabling AAA RADIUS accounting-on (extended), [33](#)
- enabling AAA RADIUS session-control, [54](#)
- enabling AAA RADIUS SNMP notification, [35](#)
- enabling APR application statistics, [476](#)
- enabling IPsec ACL de-encapsulated packet check, [304](#)

- enabling IPsec IKE invalid SPI recovery, [340](#)
- enabling IPsec IKEv2 cookie challenging, [371](#)
- enabling IPsec packet logging, [307](#)
- enabling IPsec QoS pre-classify, [307](#)
- enabling IPv4 object policy rule matching acceleration, [498](#)
- enabling IPv4 source guard (IPv4SG) on interface, [538](#)
- enabling IPv6 object policy rule matching acceleration, [498](#)
- enabling IPv6 source guard (IPv6SG) on interface, [538](#)
- enabling MAC authentication, [123](#)
- enabling NETCONF-over-SSH, [397](#)
- enabling outgoing packets filtering on portal interface, [149](#)
- enabling password control, [228](#)
- enabling port security, [205](#)
- enabling port security
  - authorization-fail-offline, [212](#)
- enabling port security MAC move, [211](#)
- enabling portal authorization strict-checking mode, [148](#)
- enabling security portal authentication, [141](#)
- enabling security portal authentication roaming, [154](#)
- enabling session management statistics collection, [482](#)
- enabling SSH SCP server, [397](#)
- enabling SSH Secure Telnet server, [396](#)
- enabling SSH SFTP server, [396](#)
- entering FIPS mode (automatic reboot), [580](#)
- entering FIPS mode (manual reboot), [580](#)
- entering peer public key, [239](#), [240](#)
- establishing SSH SCP server connection, [412](#)
- establishing SSH SCP server connection based on Suite B, [415](#)
- establishing SSH Secure Telnet server connection, [403](#)

- establishing SSH Secure Telnet server connection based on Suite B, [406](#)
- establishing SSH SFTP server connection, [407](#)
- establishing SSH SFTP server connection based on Suite B, [409](#)
- exiting FIPS mode, [582](#)
- exiting FIPS mode (automatic reboot), [582](#)
- exiting FIPS mode (manual reboot), [582](#)
- exporting host public key, [238](#)
- exporting PKI certificate, [256](#)
- generating SCP client local DSA key pair, [411](#)
- generating SCP client local RSA key pair, [411](#)
- generating SFTP client local DSA key pair, [406](#)
- generating SFTP client local RSA key pair, [406](#)
- generating SSH server local DSA key pair, [395](#)
- generating SSH server local RSA key pair, [395](#)
- generating Stelnet client local DSA key pair, [402](#)
- generating Stelnet client local RSA key pair, [402](#)
- ignoring port security server authorization information, [211](#)
- implementing security ACL-based IPsec, [292](#)
- importing peer public key from file, [239](#)
- importing public key from file, [242](#)
- interpreting AAA RADIUS class attribute as CAR parameter, [33](#)
- limiting port security secure MAC addresses, [206](#)
- logging out security portal authentication users, [155](#)
- maintaining 802.1X, [106](#)
- maintaining AAA HWTACACS, [41](#)
- maintaining AAA RADIUS, [35](#)
- maintaining APR, [477](#)
- maintaining ARP detection, [557](#)
- maintaining ASPF, [467](#)
- maintaining attack D&P, [523](#)
- maintaining connection limit, [488](#)
- maintaining crypto engine, [578](#)
- maintaining IP source guard (IPSG), [539](#)
- maintaining IPsec, [313](#)



maintaining IPsec IKE, [342](#)  
maintaining IPsec IKEv2, [372](#)  
maintaining IPv4 source guard (IPv4SG), [539](#)  
maintaining IPv6 source guard (IPv6SG), [539](#)  
maintaining MAC authentication, [127](#)  
maintaining mGRE, [594](#)  
maintaining security password control, [232](#)  
maintaining security portal authentication, [156](#)  
maintaining session management, [483](#)  
obtaining PKI certificate, [253](#)  
referencing security portal authentication Web server, [142](#)  
removing PKI certificate, [257](#)  
requesting PKI certificate request, [251](#)  
setting 802.1X authentication request attempts max, [98](#)  
setting 802.1X authentication timeout timers, [98](#)  
setting 802.1X concurrent port users max, [98](#)  
setting 802.1X port authorization state, [96](#)  
setting 802.1X quiet timer, [101](#)  
setting AAA concurrent login user max, [56](#)  
setting AAA HWTACACS timer, [40](#)  
setting AAA HWTACACS traffic statistics unit, [39](#)  
setting AAA HWTACACS username format, [39](#)  
setting AAA LDAP server timeout period, [43](#)  
setting AAA RADIUS Remanent\_Volume attribute data measurement unit, [34](#)  
setting AAA RADIUS request transmission attempts max, [29](#)  
setting AAA RADIUS server status, [29](#)  
setting AAA RADIUS timer, [31](#)  
setting AAA RADIUS traffic statistics unit, [28](#)  
setting AAA RADIUS username format, [28](#)  
setting MAC authentication concurrent port users max, [125](#)  
setting password control parameters (global), [229](#)

setting password control parameters (local user), [231](#)  
setting password control parameters (super), [231](#)  
setting password control parameters (user group), [230](#)  
setting port security mode, [206](#)  
setting security portal authentication max number users, [145](#)  
setting session management aging time (application layer protocol), [481](#)  
setting session management aging time (protocol state), [480](#)  
specifying 802.1X access control method, [97](#)  
specifying 802.1X mandatory port authentication domain, [100](#)  
specifying 802.1X supported domain name delimiters, [103](#)  
specifying AAA HWTACACS accounting server, [37](#)  
specifying AAA HWTACACS authentication server, [36](#)  
specifying AAA HWTACACS authorization server, [37](#)  
specifying AAA HWTACACS outgoing packet source IP address, [39](#)  
specifying AAA HWTACACS scheme VPN, [38](#)  
specifying AAA HWTACACS shared keys, [38](#)  
specifying AAA LDAP attribute map for authorization, [45](#)  
specifying AAA LDAP authentication server, [45](#)  
specifying AAA LDAP authorization server, [45](#)  
specifying AAA LDAP version, [42](#)  
specifying AAA RADIUS accounting server parameters, [27](#)  
specifying AAA RADIUS authentication server, [26](#)  
specifying AAA RADIUS outgoing packet source IP address, [30](#)  
specifying AAA RADIUS scheme VPN, [28](#)  
specifying AAA RADIUS shared keys, [28](#)

- specifying an attribute version for AAA HUAWEI RADIUS attributes 26-1 and 26-4 interpretation, [35](#)
- specifying MAC authentication domain, [123](#)
- specifying NAS-Port-ID attribute format, [154](#)
- specifying PKI CA storage path, [256](#)
- specifying security portal authentication domain, [146](#)
- specifying security portal preauthentication domain, [147](#)
- specifying session management persistent session, [482](#)
- specifying SSH Secure Telnet packet source IP address, [402](#)
- specifying SSH server PKI domain, [401](#)
- specifying SSH SFTP packet source IP address, [407](#)
- specifying SSH2 algorithms, [415](#)
- terminating SSH SFTP server connection, [411](#)
- triggering FIPS self-test, [584](#)
- troubleshooting 802.1X, [119](#)
- troubleshooting AAA LDAP user authentication fails, [78](#)
- troubleshooting AAA RADIUS accounting error, [77](#)
- troubleshooting AAA RADIUS authentication failure, [76](#)
- troubleshooting AAA RADIUS packet delivery failure, [77](#)
- troubleshooting connection limit overlapping ACL segments, [491](#)
- troubleshooting IPsec IKE negotiation failure (no proposal match), [358](#)
- troubleshooting IPsec IKE negotiation failure (no proposal or keychain specified correctly), [358](#)
- troubleshooting IPsec IKEv2 negotiation failure (no proposal match), [390](#)
- troubleshooting IPsec SA negotiation failure (invalid identity info), [359](#)

- troubleshooting IPsec SA negotiation failure (no transform set match), [359](#), [390](#)
- troubleshooting IPsec SA negotiation failure (tunnel failure), [391](#)
- troubleshooting PKI CA certificate import failure, [283](#)
- troubleshooting PKI CA certificate obtain failure, [281](#)
- troubleshooting PKI certificate export failure, [284](#)
- troubleshooting PKI CRL obtain failure, [283](#)
- troubleshooting PKI local certificate import failure, [284](#)
- troubleshooting PKI local certificate obtain failure, [281](#)
- troubleshooting PKI local certificate request failure, [282](#)
- troubleshooting PKI storage path set failure, [285](#)
- troubleshooting port security mode cannot be set, [222](#)
- troubleshooting port security secure MAC addresses, [222](#)
- troubleshooting security 802.1X EAD assistant Web browser users not correctly redirected, [119](#)
- troubleshooting security portal authentication cannot log out users (access device), [199](#)
- troubleshooting security portal authentication cannot log out users (RADIUS server), [200](#)
- troubleshooting security portal authentication no page pushed for users, [199](#)
- troubleshooting security portal authentication users cannot log in (re-DHCP), [200](#)
- troubleshooting security portal authentication users logged out still exist on server, [200](#)
- verifying PKI certificate, [254](#)
- verifying PKI certificate verification (CRL checking), [254](#)
- verifying PKI certificate verification (w/o CRL checking), [255](#)
- working with SSH SFTP directories, [410](#)
- working with SSH SFTP files, [410](#)



## process

AAA LDAP authentication process, [10](#)

AAA LDAP authorization process, [11](#)

## profile

AAA NAS-ID profile configuration, [57](#)

AAA RADIUS server status detection test profile, [25](#)

IPsec application to tunnel interface (IKE-based), [312](#)

IPsec IKE configuration, [334](#)

IPsec IKEv2 configuration, [365](#)

IPsec IPv6 routing protocol profile (manual), [309](#)

IPsec profile (IKE-based), [311](#)

## proposal

IPsec IKE proposal, [336](#)

IPsec IKEv2 proposal, [369](#)

## protecting

ARP attack protection configuration, [546](#)

ARP gateway protection, [561](#)

## protocols and standards

802.1X overview, [79](#)

802.1X related protocols, [80](#)

AAA, [14](#)

AAA HWTACACS, [7](#), [14](#)

AAA LDAP, [9](#), [14](#)

AAA RADIUS, [2](#), [14](#)

ASPF inspection, [463](#)

IPsec, [291](#)

IPsec IKE, [333](#)

IPsec IKEv2, [364](#)

IPsec IPv6 routing protocols configuration, [309](#)

IPsec security protocol 50 (ESP), [286](#)

IPsec security protocol 51 (AH), [286](#)

SSL configuration, [455](#), [456](#)

SSL protocol stack, [455](#)

## public key

display, [240](#)

file import, [242](#)

FIPS compliance, [236](#)

host public key display, [238](#)

host public key export, [238](#)

local host public key distribution, [237](#)

local key pair creation, [236](#)

local key pair destruction, [238](#)

management, [236](#), [240](#)

peer configuration, [239](#)

peer public key entry, [239](#), [240](#)

peer public key import from file, [239](#)

SSH client host public key configuration, [398](#)

SSH password-publickey authentication, [393](#)

SSH publickey authentication, [393](#)

SSH Secure Telnet client publickey authentication, [429](#)

SSH Secure Telnet server publickey authentication, [420](#)

SSH SFTP client publickey authentication, [437](#)

SSH user configuration, [399](#)

Public Key Infrastructure. Use [PKI](#)

## Q

### QoS

APR configuration, [474](#)

IPsec QoS pre-classify enable, [307](#)

### quiet

802.1X timer, [101](#)

MAC authentication quiet timer, [124](#)

## R

### RA

PKI architecture, [246](#)

PKI certificate, [245](#)

### RADIUS

802.1X EAP over RADIUS, [81](#)

802.1X EAP relay enable, [96](#)

802.1X EAP termination enable, [96](#)

802.1X RADIUS EAP-Message attribute, [81](#)

- 802.1X RADIUS Message-Authentication attribute, [82](#)
- AAA configuration, [1](#), [18](#), [58](#)
- AAA implementation, [2](#)
- AAA local user configuration, [20](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA scheme, [19](#)
- accounting server parameters, [27](#)
- accounting-on enable, [32](#)
- accounting-on enable (extended), [33](#)
- Acct-Session-Id format, [57](#)
- applying interface NAS-ID profile, [156](#)
- attributes, [15](#)
- authentication server, [26](#)
- class attribute as CAR parameter, [33](#)
- client/server model, [2](#)
- common standard attributes, [15](#)
- DAE server, [55](#)
- display, [35](#)
- extended attributes, [6](#)
- Hewlett Packard Enterprise proprietary attributes, [16](#)
- HUAWEI attributes 26-1 and 26-4 interpretation (version 1.0), [35](#)
- HUAWEI attributes 26-1 and 26-4 interpretation (version 1.1), [35](#)
- HWTACACS/RADIUS differences, [7](#)
- information exchange security, [2](#)
- Login-Service attribute check method, [34](#)
- MAC authentication, [120](#)
- MAC authentication (RADIUS-based), [129](#)
- maintain, [35](#)
- outgoing packet source IP address, [30](#)
- packet DSCP priority change, [55](#)
- packet exchange process, [3](#)
- packet format, [3](#)
- port security macAddressWithRadius, [204](#)
- port security NAS-ID profile, [212](#)
- protocols and standards, [14](#)

- real-time accounting timer, [31](#)
- Remanent\_Volume attribute data measurement unit, [34](#)
- request transmission attempts max, [29](#)
- scheme configuration, [25](#)
- scheme creation, [26](#)
- scheme VPN specification, [28](#)
- security policy server IP address, [33](#)
- server quiet timer, [31](#)
- server response timeout timer, [31](#)
- server SSH user authentication+authorization, [58](#)
- server status, [29](#)
- server status detection test profile, [25](#)
- session-control, [54](#)
- shared keys, [28](#)
- SNMP notification enable, [35](#)
- traffic statistics units, [28](#)
- troubleshooting, [76](#)
- troubleshooting accounting error, [77](#)
- troubleshooting authentication failure, [76](#)
- troubleshooting packet delivery failure, [77](#)
- troubleshooting security portal authentication cannot log out users (RADIUS server), [200](#)
- user authentication methods, [2](#)
- username format, [28](#)

#### real-time

- AAA HWTACACS real-time accounting timer, [40](#)
- AAA RADIUS real-time accounting timer, [31](#)

#### rebooting

- FIPS mode (automatic reboot), [587](#)
- FIPS mode (manual reboot), [587](#)
- FIPS mode entry (manual reboot), [585](#)

#### record protocol (SSL), [455](#)

#### recovering

- IPsec IKE invalid SPI recovery, [340](#)

#### re-DHCP portal authentication mode, [136](#), [138](#)

#### redundancy

- IPsec anti-replay redundancy, [305](#)

#### referencing

- security portal authentication Web server, [142](#)
- registrating
  - mGRE registration, [589](#)
- registration authority. *Use* [RA](#)
- relay agent
  - 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
  - authorized ARP (DHCP relay agent), [553](#)
- remote
  - 802.1X authorization VLAN, [88](#)
  - AAA remote accounting method, [13](#)
  - AAA remote authentication, [13](#)
  - AAA remote authentication configuration, [18](#)
  - AAA remote authorization method, [13](#)
- Remote Authentication Dial-In User Service. *Use* [RADIUS](#)
- removing
  - PKI certificate, [257](#)
- request
  - PKI certificate request abort, [253](#)
- requesting
  - PKI certificate request, [251](#)
- resource access restriction (portal authentication), [134](#)
- restrictions
  - ARP detection restricted forwarding, [556](#), [558](#)
  - ARP scanning configuration, [560](#)
  - FIPS configuration, [579](#)
  - fixed ARP configuration, [560](#)
  - IPsec policy configuration (IKE-based), [299](#)
  - IPsec policy configuration restrictions, [297](#)
  - Secure Telnet client local key pair generation, [402](#)
  - security portal authentication, [142](#)
  - SSH SCP client local key pair generation, [411](#)
  - SSH server local key pair generation, [396](#)
  - SSH SFTP client local key pair generation, [407](#)
  - SSH user configuration, [399](#)
  - user profile configuration, [224](#)
- retransmission
  - IPsec IKEv2, [364](#)
- reverse route injection. *Use* [RRI](#)
- Revest-Shamir-Adleman Algorithm. *Use* [RSA](#)
- RIP
  - mGRE routing configuration, [593](#)
- RIPng
  - IPsec RIPng configuration, [324](#)
- roaming
  - security portal authentication roaming, [154](#)
- route
  - IPsec RRI, [290](#)
  - IPsec RRI configuration, [308](#)
- router
  - APR configuration, [478](#)
  - portal authentication direct, [157](#)
  - portal authentication re-DHCP, [167](#)
  - security portal authentication, [157](#)
- routing
  - 802.1X authentication configuration, [106](#)
  - 802.1X basic configuration, [106](#)
  - 802.1X configuration, [88](#), [95](#)
  - 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
  - 802.1X EAD assistant configuration (DHCP server), [115](#)
  - 802.1X guest VLAN assignment configuration, [108](#)
  - 802.1X+ACL assignment configuration, [111](#)
  - APR application group configuration, [476](#)
  - APR PBAR configuration, [475](#)
  - IPsec IPv6 routing protocol profile (manual), [309](#)
  - IPsec IPv6 routing protocols configuration, [309](#)
  - mGRE configuration, [593](#)
  - mGRE route learning, [591](#)
  - SSH configuration, [392](#)
  - SSH server configuration, [395](#)
- RRI

configuration, [308](#)

IPsec RRI configuration, [327](#)

## RSA

IPsec IKE configuration (aggressive mode+RSA signature authentication), [346](#)

IPsec IKE signature authentication, [332](#)

PKI certificate export, [256](#)

PKI Keon CA server certificate request (NAT-PT network), [268](#)

PKI OpenCA server certificate request, [265](#)

PKI RSA Keon CA server certificate request, [259](#)

PKI Windows 2003 CA server certificate request, [261](#)

PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)

public key management, [236](#), [240](#)

SCP client RSA host key pair, [411](#)

SCP client RSA server key pair, [411](#)

SFTP client RSA host key pair, [406](#)

SFTP client RSA server key pair, [406](#)

SSH client host public key configuration, [398](#)

SSH management parameters, [400](#)

SSH Secure Telnet server publickey authentication, [420](#)

SSH server RSA host key pair, [395](#)

SSH server RSA server key pair, [395](#)

SSH SFTP client publickey authentication, [437](#)

Stelnet client RSA host key pair, [402](#)

Stelnet client RSA server key pair, [402](#)

RST flood attack, [515](#)

## rule

connection limit per-destination, [487](#)

connection limit per-service, [487](#)

connection limit per-source, [487](#)

IPsec ACL rule keywords, [292](#)

object policy, [495](#)

object policy configuration, [495](#), [499](#)

object policy rule configuration, [496](#)

object policy rule description, [495](#)

object policy rule match order, [495](#)

object policy rule match order change, [498](#)

object policy rule matching acceleration, [498](#)

object policy rule numbering, [495](#)

security portal authentication portal-free rule, [143](#)

## S

S/MIME (PKI secure email), [247](#)

## SA

IPsec transform set, [295](#)

security IKE SA max, [341](#)

troubleshooting IPsec SA negotiation failure (invalid identity info), [359](#)

troubleshooting IPsec SA negotiation failure (no transform set match), [359](#), [390](#)

troubleshooting IPsec SA negotiation failure (tunnel failure), [391](#)

## SA rekeying

IPsec IKEv2, [364](#)

## scanning attack

attack D&P defense policy, [513](#)

attack D&P device-preventable attacks, [503](#), [505](#)

## scheme

AAA, [19](#)

AAA HWTACACS, [36](#)

AAA HWTACACS scheme VPN, [38](#)

AAA LDAP, [42](#)

AAA LDAP scheme creation, [45](#)

AAA RADIUS, [25](#)

AAA RADIUS scheme VPN, [28](#)

## SCP

client device configuration, [411](#)

client local key pair generation restrictions, [411](#)

configuration, [444](#)

configuration (Suite B), [446](#)

file transfer+password authentication, [444](#)

server connection establishment, [412](#)

- server connection establishment based on Suite B, [415](#)
- server enable, [397](#)
- SSH application, [392](#)

secure shell. Use [SSH](#)

Secure Sockets Layer. Use [SSL](#)

Secure Telnet

- client device configuration, [402](#)
- client local key pair generation restrictions, [402](#)
- client password authentication, [425](#)
- client publickey authentication, [429](#)
- configuration, [417](#)
- configuration (128-bit Suite B), [431](#)
- server connection establishment, [403](#)
- server connection establishment based on Suite B, [406](#)
- server password authentication, [417](#)
- server publickey authentication, [420](#)
- SSH application, [392](#)
- SSH packet source IP address, [402](#)

security

- 802.1X access control method, [97](#)
- 802.1X authentication, [82](#), [83](#)
- 802.1X authentication configuration, [106](#)
- 802.1X authentication request attempts max, [98](#)
- 802.1X authentication server timeout timer, [98](#)
- 802.1X authentication trigger, [100](#)
- 802.1X Auth-Fail VLAN, [91](#), [102](#)
- 802.1X authorization VLAN, [88](#)
- 802.1X authorization VLAN assignment configuration, [108](#)
- 802.1X basic configuration, [106](#)
- 802.1X critical VLAN, [91](#), [103](#)
- 802.1X display, [106](#)
- 802.1X EAD assistant, [104](#)
- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)

- 802.1X EAD assistant configuration (DHCP server), [115](#)

- 802.1X EAP relay enable, [96](#)

- 802.1X EAP termination enable, [96](#)

- 802.1X enable, [95](#)

- 802.1X guest VLAN, [90](#), [102](#)

- 802.1X guest VLAN assignment configuration, [108](#)

- 802.1X maintain, [106](#)

- 802.1X mandatory port authentication domain, [100](#)

- 802.1X online user handshake, [99](#)

- 802.1X overview, [79](#)

- 802.1X periodic online user reauthentication, [101](#)

- 802.1X port authorization state, [96](#)

- 802.1X port users max, [98](#)

- 802.1X related protocols, [80](#)

- 802.1X SmartOn, [105](#)

- 802.1X SmartOn feature configuration, [117](#)

- 802.1X supported domain name delimiters, [103](#)

- 802.1X+ACL assignment configuration, [111](#)

- AAA concurrent login user max, [56](#)

- AAA configuration, [1](#), [18](#), [58](#)

- AAA device implementation, [12](#)

- AAA display, [58](#)

- AAA HWTACACS implementation, [7](#)

- AAA HWTACACS scheme, [36](#), [36](#)

- AAA HWTACACS server SSH users, [63](#)

- AAA ISP domain accounting method, [52](#)

- AAA ISP domain attribute, [47](#)

- AAA ISP domain authentication method, [49](#)

- AAA ISP domain authorization method, [51](#)

- AAA ISP domain creation, [46](#)

- AAA ISP domain method, [46](#)

- AAA ITA policy configuration, [56](#)

- AAA LDAP implementation, [9](#)

- AAA LDAP scheme, [42](#)

- AAA LDAP server SSH user authentication, [65](#)

- AAA LDAP server SSL VPN user authentication+authorization, [70](#)
- AAA local SSH user authentication+authorization, [62](#)
- AAA local user, [20](#)
- AAA MPLS L3VPN implementation, [14](#)
- AAA protocols and standards, [14](#)
- AAA RADIUS Acct-Session-Id format, [57](#)
- AAA RADIUS attributes, [15](#)
- AAA RADIUS DAE server, [55](#)
- AAA RADIUS implementation, [2](#)
- AAA RADIUS information exchange security mechanism, [2](#)
- AAA RADIUS packet DSCP priority, [55](#)
- AAA RADIUS scheme, [25](#)
- AAA RADIUS security policy server IP address, [33](#)
- AAA RADIUS server SSH user authentication+authorization, [58](#)
- AAA RADIUS server status detection test profile, [25](#)
- AAA RADIUS session-control, [54](#)
- AAA scheme, [19](#)
- APR application group configuration, [476](#)
- APR application statistics enable, [476](#)
- APR configuration, [474](#), [478](#)
- APR display, [477](#)
- APR maintain, [477](#)
- ARP active acknowledgement, [551](#)
- ARP attack detection (source MAC-based), [549](#), [550](#)
- ARP attack protection (unresolvable IP attack), [547](#), [548](#)
- ARP attack protection blackhole routing (unresolvable IP attack), [547](#)
- ARP attack protection configuration, [546](#)
- ARP attack protection source suppression (unresolvable IP attack), [547](#)
- ARP detection configuration, [554](#)
- ARP detection display, [557](#)

- ARP detection maintain, [557](#)
- ARP detection packet validity check, [556](#)
- ARP detection restricted forwarding, [556](#), [558](#)
- ARP detection user validity check configuration, [555](#)
- ARP detection user+packet validity check, [557](#)
- ARP filtering, [562](#), [563](#)
- ARP gateway protection, [561](#), [561](#)
- ARP packet source MAC consistency check, [551](#)
- ARP scanning, [560](#)
- ARP scanning configuration restrictions, [560](#)
- ASPF, [465](#)
- ASPF application inspection (FTP), [467](#)
- ASPF application inspection (H.323), [470](#)
- ASPF application inspection (TCP), [468](#)
- ASPF configuration, [462](#), [465](#), [467](#), [467](#)
- ASPF display, [467](#)
- ASPF maintain, [467](#)
- ASPF policy application (interface), [466](#)
- ASPF policy application (zone pair), [466](#), [471](#)
- association. See [SA](#)
- attack D&P blacklist, [506](#)
- attack D&P blacklist configuration, [531](#)
- attack D&P client verification, [507](#)
- attack D&P client verification (DNS), [509](#)
- attack D&P client verification (HTTP), [510](#)
- attack D&P client verification (TCP), [507](#)
- attack D&P client verification configuration (DNS), [533](#)
- attack D&P client verification configuration (HTTP), [534](#)
- attack D&P client verification configuration (TCP), [532](#)
- attack D&P command and hardware compatibility, [503](#)
- attack D&P configuration, [503](#), [511](#), [528](#)
- attack D&P configuration (interface-based), [528](#)
- attack D&P defense policy, [511](#)
- attack D&P detection exemption, [518](#)

- attack D&P device-preventable attacks, 503
- attack D&P display, 523
- attack D&P log aggregation, 520
- attack D&P maintain, 523
- attack D&P policy application (device), 519
- attack D&P policy application (interface), 519
- authorized ARP (DHCP relay agent), 553
- authorized ARP (DHCP server), 552
- authorized ARP configuration, 551
- configuring preauthentication IP address pool for portal user, 148
- connection limit configuration, 486, 489
- connection limit configuration (interface-based), 486
- connection limit display, 488
- connection limit maintain, 488
- connection limit policy application, 488
- connection limit policy configuration, 487
- connection limit policy creation, 487
- crypto engine configuration, 577
- crypto engine display, 578
- crypto engine hardware configuration, 577
- crypto engine maintain, 578
- enabling portal authorization strict-checking, 148
- expired password login, 226
- FIPS configuration, 579, 584
- FIPS configuration restrictions, 579
- FIPS display, 584
- FIPS mode configuration, 580
- FIPS mode entry, 580
- FIPS mode entry (automatic reboot), 584
- FIPS mode entry (manual reboot), 585
- FIPS mode exit, 582
- FIPS mode exit (automatic reboot), 587
- FIPS mode exit (manual reboot), 587
- FIPS mode system changes, 581
- FIPS self-test, 583
- fixed ARP configuration, 560

- fixed ARP configuration restrictions, 560
- host public key export, 238
- HWTACACS protocols and standards, 14
- IP, 286, *See also* IPsec
- IP source guard (IPSG)
  - configuration, 536, 537, 540
- IP source guard (IPSG) dynamic binding, 537
- IP source guard (IPSG) static binding, 536
- IPsec ACL anti-replay, 305
- IPsec ACL-based implementation, 292
- IPsec configuration, 286, 314
- IPsec crypto engine, 289
- IPsec display, 313
- IPsec encapsulation modes, 286
- IPsec for mGRE tunnel configuration, 593
- IPsec IKE configuration, 331, 333, 342
- IPsec IKE display, 342
- IPsec IKE maintain, 342
- IPsec IKE mechanism, 332
- IPsec IKE profile configuration, 334
- IPsec IKE protocols and standards, 333
- IPsec IKEv2 configuration, 363, 364, 373
- IPsec IKEv2 display, 372
- IPsec IKEv2 maintain, 372
- IPsec IKEv2 new features, 364
- IPsec IKEv2 policy configuration, 368
- IPsec IKEv2 profile configuration, 365
- IPsec IKEv2 protocols and standards, 364
- IPsec IPv6 routing protocols, 309
- IPsec maintain, 313
- IPsec packet DF bit, 307
- IPsec packet logging enable, 307
- IPsec policy configuration restrictions, 297
- IPsec policy configuration restrictions (IKE-based), 299
- IPsec profile (IKE-based), 311
- IPsec profile application to tunnel interface (IKE-based), 312
- IPsec protocols, 286



IPsec protocols and standards, [291](#)  
 IPsec QoS pre-classify enable, [307](#)  
 IPsec RRI, [290](#)  
 IPsec RRI configuration, [308](#)  
 IPsec security strength, [291](#)  
 IPsec SNMP notification, [312](#)  
 IPsec tunnel configuration, [311](#)  
 IPv4 address object group configuration, [493](#)  
 IPv4 source guard (IPv4SG)  
 configuration, [537](#)  
 IPv4 source guard (IPv4SG) dynamic binding  
 configuration, [541](#)  
 IPv4 source guard (IPv4SG) dynamic  
 binding+DHCP relay configuration, [542](#)  
 IPv4 source guard (IPv4SG) enable on  
 interface, [538](#)  
 IPv4 source guard (IPv4SG) static binding  
 configuration, [538](#), [540](#)  
 IPv6 address object group configuration, [493](#)  
 IPv6 source guard (IPv6SG)  
 configuration, [538](#)  
 IPv6 source guard (IPv6SG) dynamic  
 binding+DHCPv6 snooping configuration, [544](#)  
 IPv6 source guard (IPv6SG) enable on  
 interface, [538](#)  
 IPv6 source guard (IPv6SG) static binding  
 configuration, [539](#), [543](#)  
 IPv6 uRPF configuration, [571](#), [574](#), [575](#)  
 IPv6 uRPF display, [575](#)  
 LDAP protocols and standards, [14](#)  
 local host public key distribution, [237](#)  
 local key pair creation, [236](#)  
 local key pair destruction, [238](#)  
 MAC authentication, [123](#), [127](#)  
 MAC authentication (local), [127](#)  
 MAC authentication (RADIUS-based), [129](#)  
 MAC authentication ACL  
 assignment, [121](#), [131](#)  
 MAC authentication concurrent port users  
 max, [125](#)  
 MAC authentication configuration, [120](#)  
 MAC authentication delay, [125](#), [125](#)  
 MAC authentication display, [127](#)  
 MAC authentication domain, [123](#)  
 MAC authentication enable, [123](#)  
 MAC authentication keep-online, [126](#)  
 MAC authentication maintain, [127](#)  
 MAC authentication methods, [120](#)  
 MAC authentication multi-VLAN mode, [126](#)  
 MAC authentication multi-VLAN mode  
 configuration, [126](#)  
 MAC authentication timer, [124](#)  
 MAC authentication user account format, [124](#)  
 MAC authentication user account policies, [120](#)  
 MAC authentication VLAN assignment, [121](#)  
 mGRE configuration, [589](#), [592](#), [594](#)  
 mGRE configuration (full-mesh NAT  
 traversal), [612](#)  
 mGRE configuration (full-mesh), [594](#), [601](#)  
 mGRE configuration (NHS-NHC), [598](#), [607](#)  
 mGRE NAT traversal, [592](#)  
 mGRE registration, [589](#)  
 mGRE tunnel establishment, [590](#)  
 NETCONF-over-SSH client user line, [397](#)  
 NETCONF-over-SSH configuration, [453](#)  
 NETCONF-over-SSH enable, [397](#)  
 object group configuration, [493](#)  
 object policy configuration, [495](#), [499](#)  
 object policy creation, [496](#)  
 object policy display, [499](#)  
 object policy rule, [495](#)  
 object policy rule configuration, [496](#)  
 object policy rule match order change, [498](#)  
 object policy rule matching acceleration, [498](#)  
 outgoing packets filtering on portal interface, [149](#)  
 password control configuration, [225](#), [228](#), [232](#)  
 password control display, [232](#)  
 password control enable, [228](#)  
 password control maintain, [232](#)



- password control parameters (global), [229](#)
- password control parameters (local user), [231](#)
- password control parameters (super), [231](#)
- password control parameters (user group), [230](#)
- password event logging, [227](#)
- password expiration, [226](#), [226](#)
- password history, [226](#)
- password not displayed, [227](#)
- password setting, [225](#)
- password updating, [226](#), [226](#)
- password user first login, [227](#)
- password user login control, [227](#)
- peer public key entry, [239](#), [240](#)
- peer public key import from file, [239](#)
- periodic MAC reauthentication, [121](#)
- PKI applications, [247](#)
- PKI architecture, [246](#)
- PKI CA policy, [246](#)
- PKI CA storage path, [256](#)
- PKI certificate export, [256](#)
- PKI certificate import/export, [275](#)
- PKI certificate obtain, [253](#)
- PKI certificate removal, [257](#)
- PKI certificate request, [251](#), [251](#)
- PKI certificate request (automatic), [252](#), [252](#)
- PKI certificate request (manual), [252](#)
- PKI certificate request abort, [253](#)
- PKI certificate verification, [254](#)
- PKI certificate verification (CRL checking), [254](#)
- PKI certificate verification (w/o CRL checking), [255](#)
- PKI certificate-based access control policy, [257](#), [274](#)
- PKI configuration, [245](#), [248](#), [259](#)
- PKI CRL, [245](#)
- PKI digital certificate, [245](#)
- PKI display, [258](#)

- PKI domain configuration, [249](#), [249](#)
- PKI entity configuration, [248](#), [248](#)
- PKI MPLS L3VPN support, [247](#)
- PKI OpenCA server certificate request, [265](#)
- PKI operation, [246](#)
- PKI RSA Keon CA server certificate request, [259](#)
- PKI RSA Keon CA server certificate request (NAT-PT network), [268](#)
- PKI terminology, [245](#)
- PKI Windows 2003 CA server certificate request, [261](#)
- PKI Windows 2003 CA server IKE negotiation+RSA digital signature, [271](#)
- port. See [port security](#)
- port object group configuration, [494](#)
- port security display, [213](#)
- portal authentication, [139](#)
- portal authentication (cross-subnet for MPLS L3VPN), [192](#)
- portal authentication BAS-IP, [153](#)
- portal authentication configuration, [134](#), [157](#)
- portal authentication cross-subnet, [170](#)
- portal authentication detection features, [149](#)
- portal authentication direct configuration, [157](#)
- portal authentication direct configuration with preauthentication domain, [194](#)
- portal authentication domain, [146](#)
- portal authentication extended cross-subnet configuration, [180](#)
- portal authentication extended direct configuration, [173](#)
- portal authentication extended re-DHCP, [176](#)
- portal authentication fail-permit, [153](#)
- portal authentication logout, [155](#)
- portal authentication max number users, [145](#)
- portal authentication policy server, [135](#)
- portal authentication re-DHCP, [167](#)
- portal authentication re-DHCP with preauthentication domain, [196](#)

- portal authentication roaming, [154](#)
- portal authentication security check function, [134](#)
- portal authentication server, [140](#)
- portal authentication server detection, [150](#)
- portal authentication source subnet, [144](#)
- portal authentication subnet, [145](#)
- portal authentication troubleshooting, [199](#)
- portal authentication types, [134](#)
- portal authentication user access, [143](#)
- portal authentication user online detection, [149](#)
- portal authentication user synchronization, [152](#)
- portal authentication Web server detection, [151](#)
- portal preauthentication domain, [147](#)
- public key display, [240](#)
- public key import from file, [242](#)
- public key management, [236](#), [240](#)
- public key peer configuration, [239](#)
- RADIUS protocols and standards, [14](#)
- SCP client local DSA key pair generation, [411](#)
- SCP client local RSA key pair generation, [411](#)
- Secure Telnet client user line, [397](#)
- service object group configuration, [494](#)
- session management, [479](#)
- session management aging time (application layer protocol), [481](#)
- session management aging time (protocol state), [480](#)
- session management configuration, [480](#)
- session management display, [483](#)
- session management logging, [482](#)
- session management maintain, [483](#)
- session management persistent session, [482](#)
- session management statistics collection enable, [482](#)
- SFTP client local DSA key pair generation, [406](#)
- SFTP client local RSA key pair generation, [406](#)
- SSH authentication methods, [393](#)
- SSH client host public key configuration, [398](#)
- SSH configuration, [392](#)
- SSH display, [417](#)
- SSH management parameters, [400](#)
- SSH SCP client device, [411](#)
- SSH SCP configuration, [444](#)
- SSH SCP configuration (Suite B), [446](#)
- SSH SCP file transfer+password authentication, [444](#)
- SSH SCP server connection establishment, [412](#)
- SSH SCP server connection establishment based on Suite B, [415](#)
- SSH SCP server enable, [397](#)
- SSH Secure Telnet client device, [402](#)
- SSH Secure Telnet client password authentication, [425](#)
- SSH Secure Telnet client publickey authentication, [429](#)
- SSH Secure Telnet configuration, [417](#)
- SSH Secure Telnet configuration based on (128-bit Suite B), [431](#)
- SSH Secure Telnet packet source IP address, [402](#)
- SSH Secure Telnet server connection establishment, [403](#)
- SSH Secure Telnet server connection establishment based on Suite B, [406](#)
- SSH Secure Telnet server enable, [396](#)
- SSH Secure Telnet server password authentication, [417](#)
- SSH Secure Telnet server publickey authentication, [420](#)
- SSH server configuration, [395](#)
- SSH server local DSA key pair generation, [395](#)
- SSH server local RSA key pair generation, [395](#)
- SSH server PKI domain, [401](#)
- SSH SFTP client device, [406](#)

- SSH SFTP client publickey authentication, [437](#)
- SSH SFTP configuration, [435](#)
- SSH SFTP configuration (192-bit Suite B), [440](#)
- SSH SFTP directories, [410](#)
- SSH SFTP files, [410](#)
- SSH SFTP help information display, [411](#)
- SSH SFTP packet source IP address, [407](#)
- SSH SFTP server connection establishment, [407](#)
- SSH SFTP server connection establishment based on Suite B, [409](#)
- SSH SFTP server connection termination, [411](#)
- SSH SFTP server enable, [396](#)
- SSH SFTP server password authentication, [435](#)
- SSH user configuration, [399](#)
- SSH user configuration restrictions, [399](#)
- SSH2 algorithms, [415](#)
- SSH2 algorithms (encryption ), [416](#)
- SSH2 algorithms (key exchange), [415](#)
- SSH2 algorithms (MAC), [416](#)
- SSH2 algorithms (public key), [416](#)
- SSL client policy configuration, [458](#)
- SSL configuration, [455](#), [456](#)
- SSL display, [459](#)
- SSL security services, [455](#)
- SSL server policy configuration, [456](#), [459](#)
- Stelnet client local DSA key pair generation, [402](#)
- Stelnet client local RSA key pair generation, [402](#)
- troubleshooting 802.1X, [119](#)
- troubleshooting AAA HWTACACS, [78](#)
- troubleshooting AAA LDAP user authentication fails, [78](#)
- troubleshooting AAA RADIUS, [76](#)
- troubleshooting AAA RADIUS accounting error, [77](#)

- troubleshooting AAA RADIUS authentication failure, [76](#)
- troubleshooting AAA RADIUS packet delivery failure, [77](#)
- troubleshooting IPsec IKE, [358](#)
- troubleshooting IPsec IKEv2, [390](#)
- troubleshooting PKI CA certificate failure, [281](#)
- troubleshooting PKI CA certificate import failure, [283](#)
- troubleshooting PKI certificate export failure, [284](#)
- troubleshooting PKI configuration, [281](#)
- troubleshooting PKI CRL obtain failure, [283](#)
- troubleshooting PKI local certificate failure, [281](#)
- troubleshooting PKI local certificate import failure, [284](#)
- troubleshooting PKI local certificate request failure, [282](#)
- troubleshooting PKI storage path set failure, [285](#)
- uRPF configuration, [564](#), [568](#), [569](#)
- uRPF display, [569](#)
- user profile configuration, [223](#), [224](#)
- user profile configuration restrictions, [224](#)
- user profile display, [224](#)

## security zone

- object policy configuration, [495](#), [499](#)

## server

- 802.1X authentication configuration, [106](#)
- 802.1X authentication server timeout timer, [98](#)
- 802.1X authorization VLAN assignment configuration, [108](#)
- 802.1X basic configuration, [106](#)
- 802.1X configuration, [88](#), [95](#)
- 802.1X EAD assistant configuration (DHCP relay agent), [112](#)
- 802.1X EAD assistant configuration (DHCP server), [115](#)
- 802.1X guest VLAN assignment configuration, [108](#)
- 802.1X SmartOn feature configuration, [117](#)
- 802.1X+ACL assignment configuration, [111](#)

- AAA HWTACACS quiet timer, [40](#)
- AAA HWTACACS response timeout timer, [40](#)
- AAA LDAP timeout period, [43](#)
- AAA RADIUS quiet timer, [31](#)
- AAA RADIUS response timeout timer, [31](#)
- MAC authentication server timeout timer, [124](#)
- PKI OpenCA server certificate request, [265](#)
- PKI Windows 2003 CA server certificate request, [261](#)
- port security authorization information, [211](#)
- security portal authentication AAA server, [135](#)
- security portal authentication fail-permit, [153](#)
- security portal authentication policy server, [135](#)
- security portal authentication server, [135](#), [140](#)
- security portal authentication server detection, [150](#)
- security portal authentication server detection+user synchronization, [184](#)
- security portal authentication system components, [134](#)
- security portal authentication Web server, [135](#), [141](#)
- security portal authentication Web server detection, [151](#)
- security portal authentication Web server reference, [142](#)
- SSL server policy configuration, [456](#), [459](#)

service

- object group, [493](#)
- object group configuration, [494](#)

session

- AAA RADIUS session-control, [54](#)
- management. See [session management](#)
- SCP client DSA or RSA key pairs, [411](#)
- SFTP client DSA or RSA key pairs, [406](#)
- SSH server DSA or RSA key pairs, [395](#)
- Stelnet client DSA or RSA key pairs, [402](#)

session management

- aging time (application layer protocol), [481](#)
- aging time (protocol state), [480](#)
- configuration, [479](#), [480](#)
- display, [483](#)
- functions, [479](#)
- maintain, [483](#)
- operation, [479](#)
- persistent session, [482](#)
- session logging, [482](#)
- session statistics collection enable, [482](#)

setting

- 802.1X authentication request attempts max, [98](#)
- 802.1X authentication timeout timers, [98](#)
- 802.1X port authorization state, [96](#)
- 802.1X port users max, [98](#)
- 802.1X quiet timer, [101](#)
- AAA concurrent login user max, [56](#)
- AAA HWTACACS timer, [40](#)
- AAA HWTACACS traffic statistics unit, [39](#)
- AAA HWTACACS username format, [39](#)
- AAA LDAP server timeout period, [43](#)
- AAA RADIUS Remanent\_Volume attribute data measurement unit, [34](#)
- AAA RADIUS request transmission attempts max, [29](#)
- AAA RADIUS server status, [29](#)
- AAA RADIUS timer, [31](#)
- AAA RADIUS traffic statistics unit, [28](#)
- AAA RADIUS username format, [28](#)
- IPsec IKE SA max, [341](#)
- IPsec packet DF bit set, [307](#)
- MAC authentication concurrent port users max, [125](#)
- password, [225](#)
- password control parameters (global), [229](#)
- password control parameters (local user), [231](#)
- password control parameters (super), [231](#)
- password control parameters (user group), [230](#)
- port security mode, [206](#)

- security portal authentication max number users, [145](#)
- session management aging time (application layer protocol), [481](#)
- session management aging time (protocol state), [480](#)

## SFTP

- client device configuration, [406](#)
- client local key pair generation restrictions, [407](#)
- client publickey authentication, [437](#)
- configuration, [435](#)
- configuration (192-bit Suite B), [440](#)
- directories, [410](#)
- files, [410](#)
- help information display, [411](#)
- server connection establishment, [407](#)
- server connection establishment based on Suite B, [409](#)
- server connection termination, [411](#)
- server enable, [396](#)
- server password authentication, [435](#)
- SSH application, [392](#)
- SSH management parameters, [400](#)
- SSH SFTP packet source IP address, [407](#)

## shared key

- AAA HWTACACS, [38](#)
- AAA RADIUS, [28](#)

## signature authentication (IKE), [332](#)

## single-channel protocol (ASPF), [462](#), [465](#)

## single-packet attack

- attack D&P defense policy, [511](#)
- attack D&P device-preventable attacks, [503](#)
- attack D&P log aggregation disable, [520](#)

## SmartOn

- 802.1X configuration, [105](#)
- 802.1X feature, [93](#)
- 802.1X feature configuration, [117](#)

## SNMP

- AAA RADIUS notifications, [35](#)
- IPsec IKE SNMP notification, [341](#)
- IPsec SNMP notification, [312](#)

## software

- crypto engine configuration, [577](#)

## source

- ARP attack detection (source MAC-based), [549](#), [550](#)
- ARP detection src-mac validity check, [556](#)
- security portal authentication portal-free rule, [143](#)
- security portal authentication subnet, [144](#)

## specifying

- 802.1X access control method, [97](#)
- 802.1X mandatory port authentication domain, [100](#)
- 802.1X supported domain name delimiters, [103](#)
- AAA HUAWEI RADIUS attribute version for attribute interpretation, [35](#)
- AAA HWTACACS accounting server, [37](#)
- AAA HWTACACS authentication server, [36](#)
- AAA HWTACACS authorization server, [37](#)
- AAA HWTACACS outgoing packet source IP address, [39](#)
- AAA HWTACACS scheme VPN, [38](#)
- AAA HWTACACS shared keys, [38](#)
- AAA LDAP attribute map for authorization, [45](#)
- AAA LDAP authentication server, [45](#)
- AAA LDAP authorization server, [45](#)
- AAA LDAP version, [42](#)
- AAA RADIUS accounting server parameters, [27](#)
- AAA RADIUS authentication server, [26](#)
- AAA RADIUS outgoing packet source IP address, [30](#)
- AAA RADIUS scheme VPN, [28](#)
- AAA RADIUS shared keys, [28](#)
- MAC authentication domain, [123](#)
- NAS-Port-ID attribute format, [154](#)
- PKI CA storage path, [256](#)
- security portal authentication domain, [146](#)

- security portal preauthentication domain, [147](#)
- session management persistent sessions, [482](#)
- SSH Secure Telnet packet source IP address, [402](#)
- SSH server PKI domain, [401](#)
- SSH SFTP packet source IP address, [407](#)
- SSH2 algorithms, [415](#)
- SPI
  - IPsec IKE invalid SPI recovery, [340](#)
- spoofing
  - IPv6 uRPF configuration, [571](#), [574](#), [575](#)
  - uRPF configuration, [564](#), [568](#), [569](#)
- SSH
  - AAA HWTACACS server SSH user, [63](#)
  - AAA LDAP server SSH user authentication, [65](#)
  - AAA local SSH user authentication+authorization, [62](#)
  - AAA RADIUS Login-Service attribute check method, [34](#)
  - AAA RADIUS server SSH user authentication+authorization, [58](#)
  - authentication methods, [393](#)
  - client host public key configuration, [398](#)
  - configuration, [392](#)
  - display, [417](#)
  - FIPS compliance, [395](#)
  - how it works, [392](#)
  - management parameters, [400](#)
  - NETCONF-over-SSH client user line, [397](#)
  - NETCONF-over-SSH configuration, [453](#)
  - NETCONF-over-SSH enable, [397](#)
  - protocols and standards, [394](#)
  - public key management, [236](#), [240](#)
  - SCP, [392](#)
  - SCP client device, [411](#)
  - SCP configuration, [444](#)
  - SCP configuration (Suite B), [446](#)
  - SCP file transfer+password authentication, [444](#)
  - SCP server connection establishment, [412](#)
  - SCP server connection establishment based on Suite B, [415](#)
  - SCP server enable, [397](#)
  - Secure Copy. *Use* [SCP](#)
  - Secure FTP. *Use* [SFTP](#)
  - Secure Telnet, [392](#)
  - Secure Telnet client device, [402](#)
  - Secure Telnet client password authentication, [425](#)
  - Secure Telnet client publickey authentication, [429](#)
  - Secure Telnet client user line, [397](#)
  - Secure Telnet configuration, [417](#)
  - Secure Telnet configuration (128-bit Suite B), [431](#)
  - Secure Telnet packet source IP address, [402](#)
  - Secure Telnet server connection establishment, [403](#)
  - Secure Telnet server connection establishment based on Suite B, [406](#)
  - Secure Telnet server enable, [396](#)
  - Secure Telnet server password authentication, [417](#)
  - Secure Telnet server publickey authentication, [420](#)
  - server configuration, [395](#)
  - server local key pair generation restrictions, [396](#)
  - server PKI domain, [401](#)
  - SFTP, [392](#)
  - SFTP client device, [406](#)
  - SFTP client publickey authentication, [437](#)
  - SFTP configuration, [435](#)
  - SFTP configuration (192-bit Suite B), [440](#)
  - SFTP directories, [410](#)
  - SFTP files, [410](#)
  - SFTP help information display, [411](#)
  - SFTP packet source IP address, [407](#)
  - SFTP server connection establishment, [407](#)
  - SFTP server connection establishment based on Suite B, [409](#)



- SFTP server connection termination, [411](#)
- SFTP server enable, [396](#)
- SFTP server password authentication, [435](#)
- SSH2 algorithms, [415](#)
- SSH2 algorithms (encryption), [416](#)
- SSH2 algorithms (key exchange), [415](#)
- SSH2 algorithms (MAC), [416](#)
- SSH2 algorithms (public key), [416](#)
- support for Suite B, [394](#)
- user configuration, [399](#)
- user configuration restrictions, [399](#)
- versions, [392](#)
- X.509v3 certificate, [394](#)
- SSL
  - client policy configuration, [458](#)
  - configuration, [455](#), [456](#)
  - display, [459](#)
  - FIPS compliance, [456](#)
  - PKI configuration, [245](#), [248](#), [259](#)
  - PKI Web application, [247](#)
  - protocol stack, [455](#)
  - public key management, [236](#), [240](#)
  - security services, [455](#)
  - server policy configuration, [456](#), [459](#)
- SSL VPN
  - AAA LDAP server SSL VPN user authentication+authorization, [70](#)
- static
  - IP source guard (IPSG) static binding, [536](#)
  - IPv4 source guard (IPv4SG) static binding configuration, [538](#), [540](#)
  - IPv6 source guard (IPv6SG) static binding configuration, [539](#), [543](#)
  - port security static secure MAC address, [209](#)
- statistics
  - AAA HWTACACS traffic statistics units, [39](#)
  - AAA RADIUS traffic statistics units, [28](#)
  - APR application statistics enable, [476](#)
  - connection limit configuration, [486](#), [489](#)
  - connection limit configuration (interface-based), [486](#)
  - session management statistics collection, [482](#)
- sticky
  - port security secure MAC address, [209](#)
- storage
  - PKI CA storage path, [256](#)
  - troubleshooting PKI storage path set failure, [285](#)
- strict checking mode
  - enabling on portal authorization information, [148](#)
- subnetting
  - APR PBAR host port mapping (subnet-based), [474](#)
  - security portal authentication (cross-subnet for MPLS L3VPN), [192](#)
  - security portal authentication cross-subnet, [170](#)
  - security portal authentication destination subnet, [145](#)
  - security portal authentication extended cross-subnet configuration, [180](#)
  - security portal authentication source subnet, [144](#)
- super password control parameters, [231](#)
- suppressing
  - ARP attack protection source suppression (unresolvable IP attack), [547](#)
- SYN flood, [514](#)
- SYN-ACK flood, [514](#)
- synchronizing
  - security portal authentication server detection+user synchronization, [184](#)
  - security portal authentication user synchronization, [152](#)
- system administration
  - object policy configuration, [495](#), [499](#)
- system administration
  - attack D&P blacklist, [522](#)
  - attack D&P blacklist configuration, [531](#)
  - attack D&P client verification (DNS), [521](#)
  - attack D&P client verification (HTTP), [522](#)

- attack D&P client verification (TCP), [520](#)
- attack D&P client verification configuration (DNS), [533](#)
- attack D&P client verification configuration (HTTP), [534](#)
- attack D&P client verification configuration (TCP), [532](#)
- attack D&P configuration, [503](#), [511](#), [528](#)
- attack D&P configuration (interface-based), [528](#)
- attack D&P defense policy, [511](#)
- attack D&P detection exemption, [518](#)
- attack D&P log aggregation, [520](#)
- attack D&P policy application (device), [519](#)
- attack D&P policy application (interface), [519](#)
- attack D&P TCP fragment attack prevention, [520](#)
- FIPS configuration, [579](#), [584](#)
- FIPS mode configuration, [580](#)
- FIPS mode entry (automatic reboot), [584](#)
- FIPS mode entry (manual reboot), [585](#)
- FIPS mode exit (automatic reboot), [587](#)
- FIPS mode exit (manual reboot), [587](#)
- FIPS mode system changes, [581](#)
- IPsec authentication, [288](#)
- IPsec configuration, [286](#)
- IPsec encryption, [288](#)
- IPsec IKE configuration, [331](#), [333](#), [342](#)
- IPsec IKE global identity information, [338](#)
- IPsec IKE invalid SPI recovery, [340](#)
- IPsec IKE keychain, [337](#)
- IPsec IKE proposal, [336](#)
- IPsec IKE SA max, [341](#)
- IPsec IKE SNMP notification, [341](#)
- IPsec IKEv2 address pool, [372](#)
- IPsec IKEv2 configuration, [363](#), [364](#), [373](#)
- IPsec IKEv2 cookie challenging, [371](#)
- IPsec IKEv2 global parameters, [371](#)
- IPsec IKEv2 keychain, [370](#)

- IPsec IKEv2 proposal, [369](#)
- password control configuration, [225](#), [228](#), [232](#)
- SCP client local key pair generation, [411](#)
- SFTP client local key pair generation, [406](#)
- SSH authentication methods, [393](#)
- SSH configuration, [392](#)
- SSH server local key pair generation, [395](#)
- Stelnet client local key pair generation, [402](#)

## T

### TCP

- AAA HWTACACS implementation, [7](#)
- ASPF application inspection (TCP), [468](#)
- attack D&P TCP client verification, [507](#), [520](#)
- attack D&P TCP client verification configuration, [532](#)
- attack D&P TCP fragment attack, [506](#)
- attack D&P TCP fragment attack prevention configuration, [520](#)
- SSL configuration, [455](#), [456](#)

### Telnet

- SSH Secure Telnet client device, [402](#)
- SSH Secure Telnet client password authentication, [425](#)
- SSH Secure Telnet client publickey authentication, [429](#)
- SSH Secure Telnet configuration, [417](#)
- SSH Secure Telnet configuration (128-bit Suite B), [431](#)
- SSH Secure Telnet packet source IP address, [402](#)
- SSH Secure Telnet server connection establishment, [403](#)
- SSH Secure Telnet server connection establishment based on Suite B, [406](#)
- SSH Secure Telnet server password configuration, [417](#)
- SSH Secure Telnet server publickey authentication, [420](#)

### terminal



- AAA RADIUS Login-Service attribute check method, [34](#)
- terminating
  - SSH SFTP server connection, [411](#)
- testing
  - AAA RADIUS server status detection test profile, [25](#)
  - FIPS conditional self-test, [583](#)
  - FIPS power-up self-test, [583](#)
  - FIPS triggered self-test, [583](#)
- TFTP
  - local host public key distribution, [237](#)
- time
  - IPsec IKE negotiation (time-based lifetime), [288](#)
  - session management time-based session logging, [482](#)
- timeout
  - 802.1X authentication timeout, [98](#)
  - MAC authentication server timeout, [124](#)
- timer
  - 802.1X authentication timeout, [98](#)
  - 802.1X quiet, [101](#)
  - AAA HWTACACS real-time accounting, [40](#)
  - AAA HWTACACS server quiet, [40](#)
  - AAA HWTACACS server response timeout, [40](#)
  - AAA RADIUS real-time accounting, [31](#)
  - AAA RADIUS server quiet, [31](#)
  - AAA RADIUS server response timeout, [31](#)
  - MAC authentication offline detect, [124](#)
  - MAC authentication quiet, [124](#)
  - MAC authentication server timeout, [124](#)
- traffic
  - AAA HWTACACS traffic statistics units, [39](#)
  - AAA RADIUS traffic statistics units, [28](#)
  - IPsec configuration, [286](#), [314](#)
  - IPsec IKE negotiation (traffic-based lifetime), [288](#)
  - IPsec RIPng configuration, [324](#)
  - IPsec RRI configuration, [308](#), [327](#)
  - IPsec tunnel for IPv4 packets (IKE-based), [317](#)
  - IPsec tunnel for IPv4 packets (manual), [314](#)
  - IPsec tunnel for IPv6 packets (IKE-based), [320](#)
  - session management traffic-based session logging, [482](#)
  - transform set (IPsec), [295](#)
  - Transmission Control Protocol. Use [TCP](#)
  - transporting
    - IPsec encapsulation transport mode, [287](#)
  - trapping
    - AAA RADIUS SNMP notification, [35](#)
    - IPsec IKE SNMP notification, [341](#)
    - IPsec SNMP notification, [312](#)
  - triggering
    - 802.1X authentication trigger, [100](#)
    - FIPS self-test, [584](#)
  - troubleshooting
    - 802.1X, [119](#)
    - AAA HWTACACS, [78](#)
    - AAA LDAP user authentication fails, [78](#)
    - AAA RADIUS, [76](#)
    - AAA RADIUS accounting error, [77](#)
    - AAA RADIUS authentication failure, [76](#)
    - AAA RADIUS packet delivery failure, [77](#)
    - connection limit overlapping ACL segments, [491](#)
    - connection limits, [491](#)
    - IPsec IKE, [358](#)
    - IPsec IKE negotiation failure (no proposal match), [358](#)
    - IPsec IKE negotiation failure (no proposal or keychain specified correctly), [358](#)
    - IPsec IKEv2, [390](#)
    - IPsec IKEv2 negotiation failure (no proposal match), [390](#)
    - IPsec SA negotiation failure (invalid identity info), [359](#)

IPsec SA negotiation failure (no transform set match), [359](#), [390](#)

IPsec SA negotiation failure (tunnel failure), [391](#)

PKI CA certificate import failure, [283](#)

PKI CA certificate obtain failure, [281](#)

PKI certificate export failure, [284](#)

PKI configuration, [281](#)

PKI CRL obtain failure, [283](#)

PKI local certificate import failure, [284](#)

PKI local certificate obtain failure, [281](#)

PKI local certificate request failure, [282](#)

PKI storage path set failure, [285](#)

port security, [222](#)

port security mode cannot be set, [222](#)

port security secure MAC addresses, [222](#)

security 802.1X EAD assistant Web browser users not correctly redirected, [119](#)

security portal authentication, [199](#)

security portal authentication cannot log out users (access device), [199](#)

security portal authentication cannot log out users (RADIUS server), [200](#)

security portal authentication no page pushed for users, [199](#)

security portal authentication users cannot log in (re-DHCP), [200](#)

security portal authentication users logged out still exist on server, [200](#)

## tunnel

IPsec for mGRE tunnel configuration, [593](#)

mGRE client configuration, [592](#)

mGRE full-mesh, [590](#)

mGRE NHC-NHC, [590](#)

mGRE NHS-NHC, [590](#)

## tunneling

IPsec configuration, [286](#), [314](#)

IPsec encapsulation tunnel mode, [287](#)

IPsec RIPng configuration, [324](#)

IPsec RRI, [290](#)

IPsec RRI configuration, [308](#), [327](#)

IPsec tunnel configuration, [311](#)

IPsec tunnel establishment, [291](#)

IPsec tunnel for IPv4 packets (IKE-based), [317](#)

IPsec tunnel for IPv4 packets (manual), [314](#)

IPsec tunnel for IPv6 packets (IKE-based), [320](#)

mGRE configuration, [589](#), [592](#), [594](#)

mGRE configuration (full-mesh NAT traversal), [612](#)

mGRE configuration (full-mesh), [594](#), [601](#)

mGRE configuration (NHS-NHC), [598](#), [607](#)

## U

### UDP

AAA RADIUS implementation, [2](#)

AAA RADIUS packet format, [3](#)

AAA RADIUS request transmission attempts max, [29](#)

AAA RADIUS session-control, [54](#)

attack D&P defense policy (UDP flood), [517](#)

uncontrolled port (802.1X), [79](#)

### unicast

802.1X unicast trigger mode, [82](#), [100](#)

Unicast Reverse Path Forwarding. *Use uRPF*

### unit

RADIUS Remanent\_Volume attribute data measurement unit, [34](#)

### updating

passwords, [226](#), [226](#)

### uRPF

check modes, [564](#)

command and hardware compatibility, [568](#)

configuration, [564](#), [568](#), [569](#)

display, [569](#)

features, [564](#)

IPv6. *See* [IPv6 uRPF](#)

network application, [568](#)

operation, [565](#)

## user

- 802.1X periodic online user reauthentication, [101](#)
- 802.1X port users max, [98](#)
- AAA concurrent login user max, [56](#)
- ARP detection user validity check, [555](#)
- ARP detection user+packet validity check, [557](#)
- security portal authentication cross-subnet, [170](#)
- security portal authentication direct configuration, [157](#)
- security portal authentication direct configuration with preauthentication domain, [194](#)
- security portal authentication extended cross-subnet configuration, [180](#)
- security portal authentication extended direct configuration, [173](#)
- security portal authentication extended re-DHCP, [176](#)
- security portal authentication logout, [155](#)
- security portal authentication max number users, [145](#)
- security portal authentication re-DHCP, [167](#)
- security portal authentication re-DHCP with preauthentication domain, [196](#)
- security portal authentication roaming, [154](#)
- security portal authentication user access, [143](#)
- security portal authentication user online detection, [149](#)
- security portal authentication user synchronization, [152](#)
- SSH user configuration, [399](#)
- userLogin 802.1X authentication mode, [204](#)
- userLoginSecure 802.1X authentication mode, [204](#)
- userLoginSecureExt 802.1X authentication mode, [204](#)

- userLoginWithOUI 802.1X authentication mode, [204](#)

## user access

- IP source guard (IPSG) configuration, [536](#), [537](#), [540](#)
- IPv4 source guard (IPv4SG) dynamic binding configuration, [541](#)
- IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)
- IPv4 source guard (IPv4SG) static binding configuration, [540](#)
- IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)
- IPv6 source guard (IPv6SG) static binding configuration, [543](#)

## user account

- MAC authentication user account format, [124](#)
- MAC authentication user account policies, [120](#)

## user authentication

- password control configuration, [225](#), [228](#), [232](#)
- password control parameters (global), [229](#)
- password control parameters (local user), [231](#)
- password control parameters (super), [231](#)
- password control parameters (user group), [230](#)
- password event logging, [227](#)
- password expiration, [226](#), [226](#)
- password expired login, [226](#)
- password history, [226](#)
- password max user account idle time, [227](#)
- password not displayed, [227](#)
- password setting, [225](#)
- password updating, [226](#), [226](#)
- password user first login, [227](#)
- password user login attempt limit, [227](#)
- password user login control, [227](#)

## user management

- AAA management by ISP domains, [12](#)
- AAA management by user access types, [12](#)
- AAA user role authentication, [13](#)

## user profile

- command and hardware compatibility, [223](#)
- compatibility, [223](#)
- configuration, [223](#), [224](#)
- configuration restrictions, [224](#)
- display, [224](#)
- feature and hardware compatibility, [223](#)

## userLoginWithOUI, [215](#)

## username

- AAA HWTACACS format, [39](#)
- AAA RADIUS format, [28](#)

## V

### validity check

- ARP detection packet, [556](#)
- ARP detection user, [555](#)
- ARP detection user+packet, [557](#)

### verifying

- attack D&P client verification, [507](#)
- attack D&P client verification (DNS), [509](#), [521](#)
- attack D&P client verification (HTTP), [510](#), [522](#)
- attack D&P client verification (TCP), [507](#), [520](#)
- PKI certificate, [254](#)
- PKI certificate verification (w/o CRL checking), [255](#)
- PKI certificate with CRL checking, [254](#)

### version

- AAA LDAP, [42](#)

### version-based HUAWEI attribute interpretation (RADIUS), [35](#)

## VLAN

- 802.1X Auth-Fail VLAN, [91](#), [102](#)
- 802.1X authorization VLAN, [88](#)
- 802.1X authorization VLAN assignment configuration, [108](#)
- 802.1X critical VLAN, [91](#), [103](#)
- 802.1X guest VLAN, [90](#), [102](#)
- 802.1X guest VLAN assignment configuration, [108](#)

## 802.1X VLAN manipulation, [88](#)

## 802.1X+ACL assignment configuration, [111](#)

### IP source guard (IPSG)

#### configuration, [536](#), [537](#), [540](#)

#### IPv4 source guard (IPv4SG) dynamic binding configuration, [541](#)

#### IPv4 source guard (IPv4SG) dynamic binding+DHCP relay configuration, [542](#)

#### IPv4 source guard (IPv4SG) static binding configuration, [540](#)

#### IPv6 source guard (IPv6SG) dynamic binding+DHCPv6 snooping configuration, [544](#)

#### IPv6 source guard (IPv6SG) static binding configuration, [543](#)

#### MAC authentication VLAN assignment, [121](#)

#### port security secure MAC address, [209](#)

#### security portal authentication portal-free rule, [143](#)

#### security portal authentication roaming, [154](#)

## VPN

### AAA HWTACACS scheme VPN, [38](#)

### AAA MPLS L3VPN implementation, [14](#)

### AAA RADIUS scheme VPN, [28](#)

### IPsec configuration, [286](#), [314](#)

### IPsec RIPng configuration, [324](#)

### IPsec RRI, [290](#)

### IPsec RRI configuration, [308](#), [327](#)

### IPsec tunnel for IPv4 packets (IKE-based), [317](#)

### IPsec tunnel for IPv4 packets (manual), [314](#)

### IPsec tunnel for IPv6 packets (IKE-based), [320](#)

### mGRE configuration, [589](#), [592](#), [594](#)

### mGRE configuration (full-mesh NAT traversal), [612](#)

### mGRE configuration (full-mesh), [594](#), [601](#)

### mGRE configuration (NHS-NHC), [598](#), [607](#)

### mGRE network type, [590](#)

### PKI application, [247](#)

### security portal authentication (cross-subnet for MPLS L3VPN), [192](#)

## W

## Web

- configuring portal authentication Web redirect, [155](#)
- PKI, [247](#)
- security portal authentication, [139](#)
- security portal authentication configuration, [134](#), [157](#)
- security portal authentication cross-subnet, [170](#)
- security portal authentication direct configuration, [157](#)
- security portal authentication direct configuration with preauthentication domain, [194](#)
- security portal authentication extended cross-subnet configuration, [180](#)
- security portal authentication extended direct configuration, [173](#)
- security portal authentication extended functions, [134](#)
- security portal authentication extended re-DHCP, [176](#)
- security portal authentication re-DHCP, [167](#)
- security portal authentication re-DHCP with preauthentication domain, [196](#)
- security portal authentication server detection+user synchronization, [184](#)
- security portal authentication system components, [134](#)
- security portal authentication Web server, [135](#), [141](#)
- security portal authentication Web server detection, [151](#)
- security portal authentication Web server reference, [142](#)
- troubleshooting 802.1X EAD assistant browser users not correctly redirected, [119](#)

## Windows 2000

- PKI CA server SCEP add-on, [248](#)
- PKI entity configuration, [248](#)

## Windows 2003

- PKI CA server certificate request, [261](#)

## Windows 2003 CA

- PKI CA server IKE negotiation+RSA digital signature, [271](#)

## WLAN

- 802.1X overview, [79](#)
- port security client macAddressElseUserLoginSecure, [218](#)
- port security client userLoginWithOUI, [215](#)
- port security configuration, [202](#), [205](#), [213](#)
- port security MAC address autoLearn, [213](#)

## working with

- SSH SFTP directories, [410](#)
- SSH SFTP files, [410](#)

## X

### X.500

- AAA LDAP implementation, [9](#)

## Z

### zone

- ASPF destination zone, [462](#)
- ASPF policy application (zone pair), [466](#), [471](#)
- ASPF source zone, [462](#)
- ASPF zone pair, [462](#)

### zone pair

- IPv4 object policy application, [498](#)
- IPv6 object policy application, [498](#)