Hewlett Packard Enterprise

HP Switch Software

OpenFlow v1.3 Administrator Guide K/KA/KB/WB 15.18

Abstract

This document describes the general steps and individual commands for enabling OpenFlow operation on HP Switches.

Applicable Products

HP 2920 Switches (J9726A, J9728A, J9727A, J9729A)
HP 3500 Switches (J9470A, J9471A, J9472A, J9473A)
HP 3500yl Switches (J8692A, J8693A, J9310A, J9311A)
HP 3800 Switches (J9573A, J9574A, J9575A, J9576A, J9584A, J9585A, J9586A, J9587A, J9588A)
HP 5406 Switches (J9533A, J9539A)
HP 5406R Switches (J9821A, J9824A, J9823A, J9868A)
HP 5406zl Switches (J8697A, J9642A, J8699A, J9447A)
HP 5412 Switches (J9532A, J9540A)
HP 5412R Switches (J9822A, J9826A, J9825A)
HP 5412zl Switches (J8698A, J9643A, J8700A, J9448A)
HP 6200yl Switch (J8992A)
HP 6600 Switches (J9263A, J9265A, J9264A, J9451A, J9452A)
HP 8206 v2 zl Switch (J9640A)
HP 8206zl Switches (J9475A, J9638A)
HP 8212zl Switches (J8715A/B, J9091A, J9641A, J9639A)

Part Number: 5998-8148b
Published: April 2016
Edition: 5

© Copyright 2016 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP 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. The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein. HP has no control over and is not responsible for information outside HP.com.

UNIX is a registered trademark of The Open Group.

Acknowledgments

This product contains OpenFlow protocol support functionality as provided in Open vSwitch code licensed under the Apache Software License v2.0 and available at **http://openvswitch.org**. The full text of the Apache Software License v2.0 is contained in the *OpenFlow License Information* document available at **www.hp.com/Networking/support**.

Warranty

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit **www.hp.com/networking/support**.

Contents

1 Introduction....7
Overview....7
OpenFlow architecture....8
Virtualization mode....8
Aggregation mode....9
OpenFlow features and benefits....10
Administrative methods....11
Supported RFCs and standards....12
Interoperability....13
Scalability....15
2 Configuring OpenFlow....16
Configuration overview....16
Entering OpenFlow....16
Entering OpenFlow context....16
Entering OpenFlow instance context....16
Preparing for configuration....16
Enabling or disabling OpenFlow....16
Setting OpenFlow protocol version....17
Configuring OpenFlow instances....17
OpenFlow instance mode....18
Configure OpenFlow instance members....18
Flow location....18
Communicating port status to the controller....19
Configuring listener ports....20
Configuring a controller....20
Associate OpenFlow instance with OpenFlow controller....21
Securing the connection between an OpenFlow instance and the controller....21
Configuring auxiliary connections....22
Associating the auxiliary connection index with an OpenFlow instance....24
Configuring number of software flow tables per instance....24
OpenFlow instance connection interruption mode....24
Setting maximum backoff interval for an instance....24
Configuring IP Control Table Mode....25
Configure OpenFlow controller ports....25
Controller roles....25
Controller role change....26
Port modification....26
Port modification and OpenFlow versions....28
Configuring egress only ports....29
Software and hardware rate limiting....30
Limiting the usage of hardware resources....30
Hardware statistics refresh rate....31
Backing up your configuration (optional)....31
Configuring VLANs....31
Configuring and verifying routing....31
Configuring physical and logical ports....31
Pipeline configuration commands....32
Validation rules....33
Openflow MAC group....33
OpenFlow pipeline....33
IP control table pipeline....34

Metadata....34
Command to configure source MAC group table on an instance....35
Validation rules....36
Destination MAC group table on an instance....37
Validation rules....38
Human readable data-path description....38
Validation table....39
3 Group table....40
OpenFlow groups in hardware....40
Group type “ALL”....40
4 OpenFlow per-flow rate limiting....42
QoS extensions....42
Create a limiter....42
Get limiter details....42
Support an OpenFlow with a limiter....42
5 OpenFlow Multi-VLAN instance....43
Overview....43
Configuration commands....43
Add member VLANs....43
Add VLANs as members to OpenFlow instance....43
Validation rules....45
Data-path description....46
Validation rules....47
Configure table number for a flow table....47
Validation rules....48
Show commands....49
Show OpenFlow information....49
Show global OpenFlow information....52
Show OpenFlow instance....52
Show OpenFlow instance group....55
Show group information for a specific instance....56
Show OpenFlow resources....56
Show OpenFlow controllers....58
Show flow table information....58
Viewing OpenFlow instance flow-table....58
Viewing global flow table information....58
Viewing specific table capability....59
Viewing group table information....61
Show meter information for a specific instance....63
v3 Push/Pop VLAN....63
Show auxiliary connection information....63
Show per flow rate limiter information....64
Show group table information....64
Viewing multiport-filter-limit....64
Show statistics....64
Viewing port statistics per instance....64
Viewing message statistics for an instance....65
Show OpenFlow instance capabilities information....65
6 OpenFlow custom pipeline....67
Custom pipeline mode....67
Default Pipeline in custom mode....68
Pipeline modification process....69
Scale on custom pipeline Instance....72

7 Administering OpenFlow....74
Setting OpenFlow statistics refresh interval....74
Refresh interval policy-engine table....74
Custom table numbering....74
Implementation notes....75
Validation rules....76
8 Troubleshooting OpenFlow....78
Diagnostic Tools Overview and Usage....78
Debug OpenFlow....78
Error messages....78
Interoperability error messages....78
Controller error messages....80
Port error messages....81
Limiter error messages....81
VLAN error messages....82
Instance error messages....83
Errors concerning auxiliary connections....84
Other scenarios....85
Troubleshooting scenarios for instances....85
Commands issued from listen port or controllers are not successful....86
Connection interruption mode setting....86
Flow modification....87
Programming flow errors....87
Flows go missing after addition....88
Missing line rate performance after flows are successfully installed....89
OpenFlow match on TCP flags & L4 port ranges....89
Matching on TCP flags and TCP/UDP port ranges....89
Experimenter match fields....89
Flow Mod Validations....90
Addition or modification of tag for single-tagged packets....90
Troubleshooting scenarios and error messages....91
How to troubleshoot if instance is not coming up....91
Reporting problems....92
9 Support and other resources....93
Contacting HP....93
Before you contact HP....93
HP contact information....93
Subscription service....93
Documents....93
Websites....94
Typographic conventions....94
Customer self repair....95
10 Documentation feedback....96
A Flow classification on v1, v2 and v3 modules....97
Hardware match chart....97
OpenFlow 1.3 multi-table model and device modes....99
B Implementation notes....101
A hardware flow with an idle timeout of 10 seconds gets deleted even though packets match the flow within the idle timeout....101
Controller flows — flow in hardware and processing software....101
DUT matches and processes incoming untagged packets for VLAN id....102
Events that change the Operational Status of the OpenFlow instance....102

OpenFlow's influence on CPU generated packets....102
OpenFlow 1.0 supports IP address masking....102
Virtualization mode verses Aggregation mode — VLAN tags in packet_in messages....103
Precedence level in meters....104
Support for miss_len field in ‘switch configuration’ messages....104
Once a controller deletes flows from Table 0, it has to re-add in order for traffic to flow through an OpenFlow switch 104
OpenFlow custom pipeline implementation notes....105
Multi-VLAN implementation notes....105
Implementation notes for OpenFlow groups in hardware....106
C Configuring secure connection HP VAN SDN controller....107
D Service Insertion....108
OpenFlow and Service Tunnels....108
Index....110

1 Introduction

This document provides the following:

- General steps for OpenFlow configuration and administration
- OpenFlow command syntax descriptions, including show commands
- OpenFlow troubleshooting commands and debug actions

This document only covers the additional features and commands for administering OpenFlow on certain HP switches that use software version 15.10 or later, as described below:

Release Version	Description
K/KA.15.10	Added OpenFlow 1.0 support for the following switches: • HP 3500, HP 3500 yl • HP 3800 • HP 5400 zl with v1 or v2 modules • HP 6200 yl • HP 6600 • HP 8200 zl with v1 and v2 modules
K/KA.15.11	Added HP QoS Extensions to OpenFlow
K/KA.15.12 and WB.15.12	Added OpenFlow support for the HP 2920
K/KA/WB 15.14	Added OpenFlow v1.3 support
K/KA/WB 15.15	GRE Tunnels support introduced for OpenFlow.
K/KA/WB 15.16	Table-0 change.
K/KA/WB 15.17	Multi-VLAN instance support, custom-match pipeline and Groups in hardware.

For more information about upgrading software, see the *Management and Configuration Guide* for your HP switch.

Overview

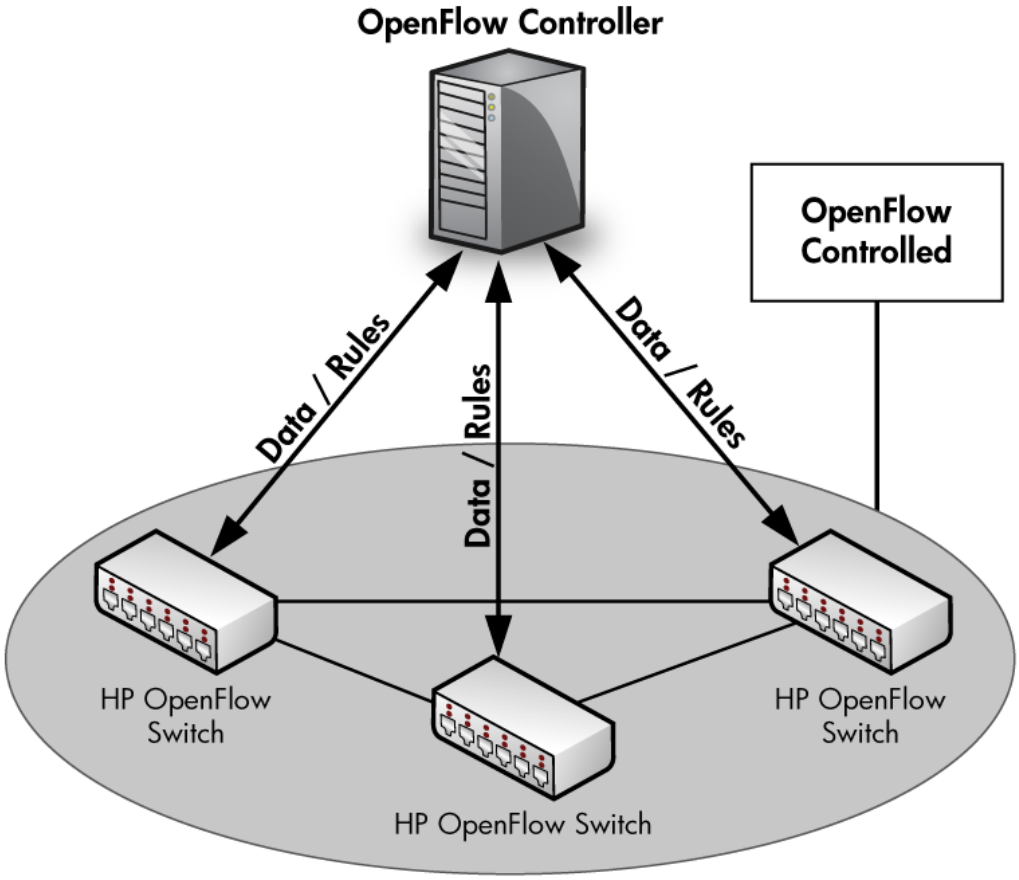
OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. OpenFlow defines a set of actions that network devices can take to manage these flows. An OpenFlow controller defines and communicates policies to specify traffic behavior on OpenFlow switches. OpenFlow separates the control plane (that decides how traffic must be forwarded) from the data plane (that implements how traffic is forwarded.)

OpenFlow is based on an Ethernet switch with internal flow-tables and a standardized interface to add and remove flow entries via an external controller.

OpenFlow is a software environment that allows for experimentation of networking protocols and traffic flows without interrupting the operation of production network. OpenFlow traffic can be separated from the rest of the traffic on the network per VLAN, so that non-OpenFlow traffic is not impacted by OpenFlow.

OpenFlow implementation on HP Switches separates OpenFlow traffic and non-OpenFlow traffic with OpenFlow instances. Traffic within an OpenFlow instance does not influence or degrade non-OpenFlow traffic. OpenFlow configuration commands are applied per-instance.

Figure 1 OpenFlow switches and controller



HP implementation complies with OpenFlow Switch Specification v1.0.0 (December 31, 2009.) With the K/KA.15.14 and WB.15.14 release, HP switches support OpenFlow Switch Specification v1.3.1 (September 2012). For implementation limitations with respect to the supported specifications, see “Supported RFCs and standards” (page 12).

For more information see the Open Networking Foundation website at **https://www.opennetworking.org/**.

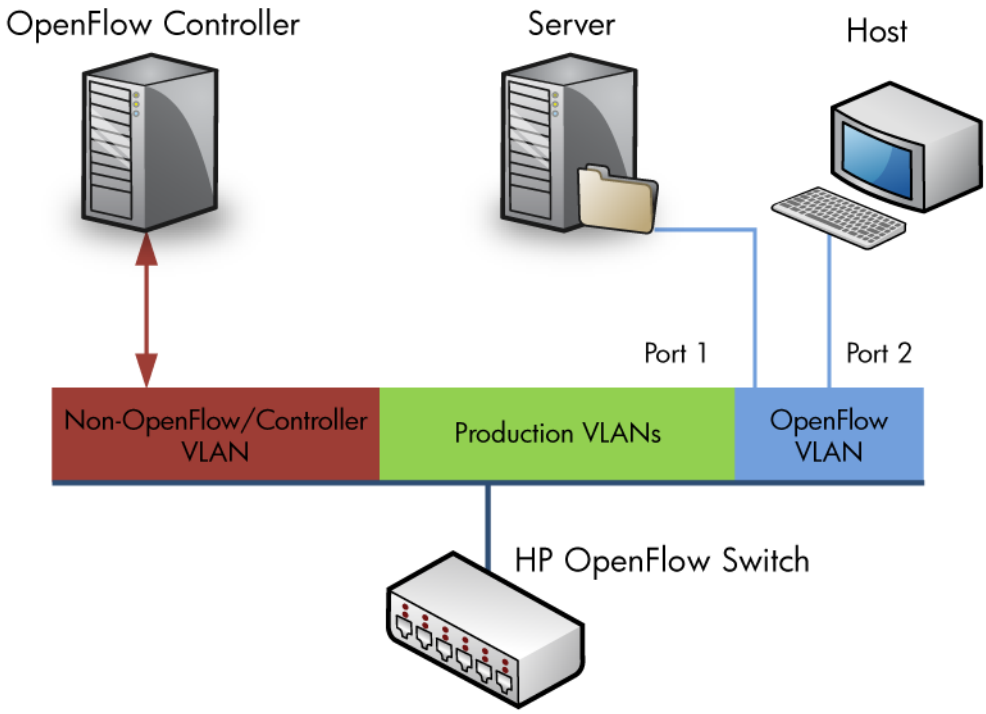
OpenFlow architecture

OpenFlow can be configured to separate non-OpenFlow traffic from OpenFlow traffic. An OpenFlow instance can either be in the Virtualization or Aggregation Mode.

Virtualization mode

Virtualization mode allows non-OpenFlow VLANs and VLANs that belong to OpenFlow instances to be configured on the switch. Each OpenFlow instance is independent and has its own OpenFlow configuration and OpenFlow controller connection. An OpenFlow instance in virtualization mode must have a VLAN associated as a member VLAN.

Figure 2 Virtualization mode



Aggregation mode

In Aggregation mode, all VLANs in the switch are part of an OpenFlow instance. The exception is the management VLAN and a VLAN that communicates to the controller. Similar to a lab environment the OpenFlow controller manages all the switching and routing for the switch.

NOTE: When Aggregation is configured, there is only OpenFlow traffic passing through the switch.

Figure 3 Aggregation mode

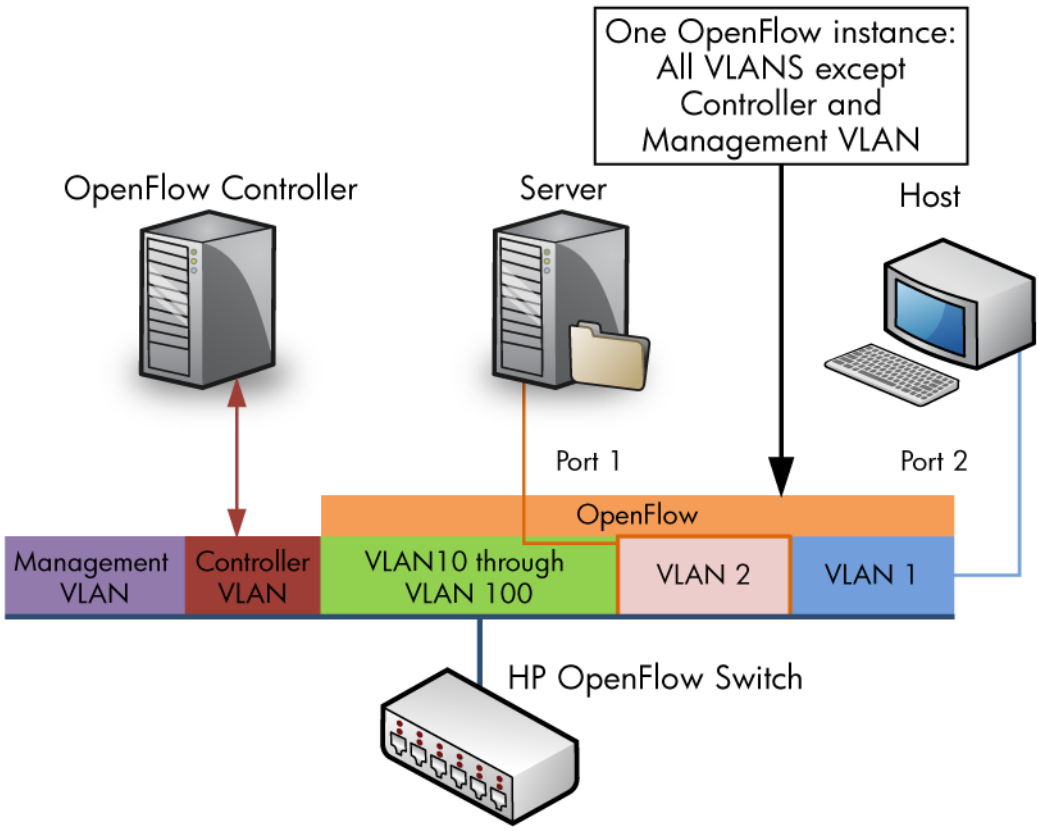
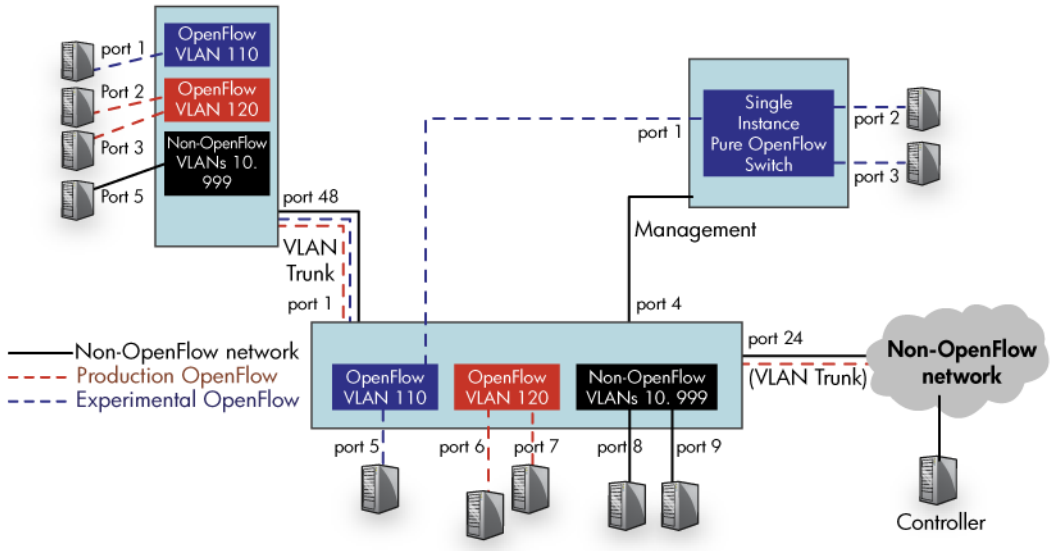


Figure 4 Example network with production non-OpenFlow, production OpenFlow, and experimental OpenFlow



OpenFlow features and benefits

With the addition of OpenFlow Specification 1.3, the following features are supported:

- Multiple Flow tables
- Pipeline processing

- Custom pipeline processing
- Multi-VLAN instances
- Groups in hardware
- OpenFlow physical, logical and reserved ports
- Version negotiation
- Group tables
- Auxiliary connections
- OpenFlow Extensible Match (OXM)
- Multiple controllers
- Support for IPv6 flows

OpenFlow switch side configuration enables the user to:

- Enable or disable OpenFlow
- Create OpenFlow instances and configure controller connections
- Display OpenFlow related configuration
- Availability of Config support to retain OpenFlow configuration across a reboot

OpenFlow supports high availability:

- The OpenFlow flow table is preserved across Management Module failover
- The OpenFlow configuration is synced from the AMM (Active Management Module) to the SMM (Standby Management Module).

OpenFlow includes tools for limiting resources:

- Support for limiting the percentage of policy engine and IP control table resources used by OpenFlow
- Support for rate-limiting the amount of OpenFlow traffic sent to the controller
- Support for rate-limiting the amount of OpenFlow traffic that gets forwarded by the policy engine rules programmed by OpenFlow

OpenFlow modes of operation:

- Support for hardware-only mode such where only flows that can be programmed into hardware are accepted from the controller.
- Support for active mode (default) where new flows are sent to the controller by the switch.
- Support for passive mode where new flows no longer are sent to the controller but are handled normally handled by the switch.

IPv6 and OpenFlow

Directing IPv6 traffic using OpenFlow is supported beginning with OpenFlow Specification 1.3. For more information on configuring IPv6 on switches, see the *IPv6 Configuration Guide* for your switch.

Administrative methods

This document provides the HP CLI commands for configuring and administering HP OpenFlow switches.

The HP VAN SDN controller has utilities for monitoring, administering, and troubleshooting OpenFlow switches. These utilities can show the current state of a switch that supports OpenFlow, including features, configuration and table entries. Other controllers have similar utilities; for example, the OpenvSwitch controller distribution includes the utility ovs-ofctl.

Supported RFCs and standards

HP switches support OpenFlow Switch Specification, version 1.0.0 (December 31, 2009) from the Open Networking Foundation, **https://www.opennetworking.org/** with some differences.

Unsupported features:

- TABLE action.
- IN_PORT action. You cannot send out the packet on the port that it arrived on.
- The “enqueue” action per the specification.
- Handling of IP Fragments: OFPC_IP_REASM/OFPC_FRAG_REASM.
- The flow emergency cache implementation.
- OpenFlow 0.8.2 - SSL controller connection.
- OpenFlow 0.8.9 - Explicit handling of IP fragments: OFPC_IP_REASM.
- OpenFlow 0.8.9 - 802.1D Spanning Tree: OpenFlow does not allow full interaction with the switch Spanning Tree. OpenFlow is confined to the switch Spanning Tree.
- OpenFlow 0.9 - Emergency Flow Cache.
- OpenFlow 0.9 - Barrier Command.
- OpenFlow 1.0 - Slicing. The hardware cannot support the slicing specification. HP provides its own QoS API instead.

Hardware acceleration limitations:

- All flows cannot be executed in the switch hardware, because of hardware limitations. Flows not executed in hardware are processed in switch software, which is a slower path.

HP switches support OpenFlow Switch Specification, version 1.3.1 (September 2012) from the Open Networking Foundation, **https://www.opennetworking.org/** with some differences.

Unsupported features:

- OFPP TABLE action.
- Set-Queue action.
- Handling of IP Fragments: OFPC_IP_REASM/OFPC_FRAG_REASM.
    - Push-MPLS, Set MPLS TTL, Decrement MPLS TTL actions
    - Push-PBB action
    - Copy TTL outwards, Copy TTL inwards actions
    - Set queue action
- Some commands for port modification from a controller:
    - OFPPC_NO_STP
    - OFPPC_NO_RECV
    - OFPPC_NO_RECV_STP
    - OFPPC_NO_FWD

NOTE: When the above port modification commands are sent from the controller, an error message is returned to the controller:

`OFPET_PORT_MOD_FAILED.`

Hardware differences between v1 & v2 Modules affect feature functionality, see “Flow classification on v1, v2 and v3 modules” (page 97) for details.

Interoperability

Table 1 HP Switch features and interoperability with OpenFlow — by effect on feature or application

Effect	Feature
Feature can override OpenFlow [1]	802.1X MAC Auth MAC Lockout MAC Lockdown Port Security Web Auth
Feature can override OpenFlow [2]	ACLs – Port, VLAN, Router, IDM variants IDM
Feature can override OpenFlow [3]	Rate Limiting
Feature can be configured if OpenFlow is used	Management VLAN **NOTE:** Management VLAN feature can be configured but it cannot be part of an OpenFlow instance.
Feature cannot be configured if OpenFlow is used [4]	Meshing Q-in-Q Remote Mirror Endpoint Transparent Mode
OpenFlow can override this feature [5]	DHCP Snooping DHCPv4 client DHCPv4 relay DHCPv6 client DNS Ping SNTP Telnet client and server TFTP TimeP Traceroute UDP broadcast forwarder
OpenFlow can override this feature [5]	BGP

Table 1 HP Switch features and interoperability with OpenFlow — by effect on feature or application *(continued)*

Effect	Feature
	DHCPv6 relay
	Dynamic ARP Protection
	Dynamic IP Lockdown
	IGMP Proxy
	IGMPv2
	IGMPv3
	MLDv1
	MLDv2
	OSPFv2
	OSPFv3
	PIM-DM
	PIM-SM
	RIP
	Static Multicast Routes
	Static Routes
	Virus Throttling
	VRRP
OpenFlow does not affect this feature	Support existing L2, L3, security, HA, QoS functionalities
OpenFlow does not affect this feature [6]	Distributed Trunking
	GVRP
	LACP
	Loop Protect
	sFlow
	UDLD
OpenFlow does not affect this feature [7]	STP loop guard
	BPDU guard
	MSTP
	RSTP
	STP
	PVST

[1] These authentication features still function in an OpenFlow instance and ports of an OpenFlow instance. The security features take a first look at the packet before sending the packets to OpenFlow.

[2] Any ACL entry that sets a drop bit in hardware (TCAM) would always win over the TCAM entry to copy OpenFlow traffic to the controller such that packets on an OpenFlow instance could get dropped in hardware due to an ACL entry and an OpenFlow controller would never be able to see those packets.

[3] Rate Limiting may be applied to limit OpenFlow traffic as well as other traffic. OpenFlow uses a form of rate-limiter to limit the OpenFlow traffic that gets to the CPU and to the controller.

[4] Enabling Meshing can break the distinction between OpenFlow VLANs and non-OpenFlow VLANs.

[5]
- The OpenFlow controller could set up a flow to match a protocol header and an action to drop the matching packets. This could lead to the protocol's packets never making it to the protocol handling code in the software data path causing the protocol to break on the OpenFlow instance.
- The OpenFlow controller could set up a flow to match a protocol header and a NORMAL action in software for the matching packets. In such a case, the protocol's packets are removed by OpenFlow in the software data path but reintroduced after examining the software flow table. Though this action may not break the protocol, it introduces an additional latency before the protocol running on the switch gets the protocol's packets.

[6] Protocol packets are not sent through the OpenFlow software data path.

[7] Port up or down events are sent to the controller to keep the controller aware of available ports on the switch. OpenFlow cannot override STP, RSTP, or MSTP decisions.

Scalability

Table 2 Switch modules scalability

Switch/Modules	Firmware version K/KA.15.10 – Flows supported	Firmware version K/KA.15.14, WB.15.14 – Flows supported
Compatible mode – "allow v1 modules" – A chassis where v1 as well as v2 modules are present may execute in this mode. Non-compatible mode – "no allow v1 modules" – A chassis that only has v2 modules may execute in this mode.		
8200/5400 v1 modules 3500 series 6600 series 6200 series	Total: 64 K	Total: 64 K
	Hardware: TCAM – 1.5K per module	Hardware: Standard match mode TCAM – 1.5 K per module
	Software: Total minus Hardware	Software: Total minus Hardware
8200/5400 v2modules 3800 series 2920 series (Flow numbers will be lower for this series)	Total: 64 K 16 K for 2920	Total: 64 K 16 K for 2920
	Hardware: TCAM - 2000 per module TCAM – 500 per module for 2920	Hardware: Compatible mode – 1.5 K per module Non-compatible mode TCAM – 4K per module
	Software: Total minus Hardware	Software: Total minus Hardware
5400R v3 modules	Compatible or non-compatible mode: 2000 rules per module — total number of rules – 64K	

2 Configuring OpenFlow

Configuration overview

1. Enable OpenFlow
2. Configure OpenFlow instances
3. Configure OpenFlow instance members
4. Set OpenFlow instance mode
5. Set Flow location
6. Configure software and hardware rate limiting
7. Configure listener ports
8. Configure controller IP and port
9. Configure policy engine resources

Entering OpenFlow

Entering OpenFlow context

You can use the `openflow` command options from configuration level by entering the word `openflow`, or from OpenFlow context level by typing the command option.

Syntax

`openflow`
Enters OpenFlow context

Entering OpenFlow instance context

You can use the `instance` *`instance-name`* command from configuration level by beginning the command with `openflow`, or from OpenFlow instance context level by typing the command option.

Syntax

`openflow instance` *`instance-name`*
Enters OpenFlow instance context
`instance-name` OpenFlow instance name

Preparing for configuration

Plan your network including production and OpenFlow VLANs, OpenFlow instances, OpenFlow controller ports, listening ports, naming and numbering strategy.

Plan the number of VLANs configured for OpenFlow versus non-OpenFlow.

OpenFlow works on an instance only when OpenFlow is enabled on the instance as well as globally on the switch.

NOTE:

A maximum of 128 OpenFlow instances can be configured. (16 on 2920)
A maximum of 2048 VLANs are supported.

Enabling or disabling OpenFlow

Enable or disable OpenFlow globally:

Syntax

```
openflow [ enable | disable ]
[no] openflow enable
```

`enable` Enables OpenFlow globally.

`disable` Disables OpenFlow globally.

NOTE: Using `no openflow` without any additional parameters deletes **all** OpenFlow configuration. A warning message to confirm this command appears.

NOTE: OpenFlow instance parameters can only be changed with OpenFlow disabled. Instance parameters cannot be changed when instance is enabled. To enable an instance use the following command.

```
openflow instance <instance name> enable
```

Setting OpenFlow protocol version

Syntax

```
openflow instance instance-name 1.0|1.3 [only]
```

Default version:1.0

OpenFlow protocol version supported by the instance.

This command lets you choose which version of OpenFlow the instance will use to negotiate with the controller. The command also allows for supported earlier versions of OpenFlow to be used in negotiation with the controller unless the option `only` is specified.

Default: version 1.0

Configuring OpenFlow instances

NOTE:

- Configuration changes are not allowed when instance is enabled. Disable the instance and make instance specific configuration changes.
- For a named instance to be enabled, a listen port or a controller, and a member VLAN have to be added to the instance.
- To enable an aggregate instance, a listen-port or a controller has to be added to the instance.

For more on Aggregation Mode, see “Aggregation mode” (page 9).

For more on Virtualization Mode, see “Virtualization mode” (page 8).

Syntax

```
openflow instance { instance-name | aggregate }[ enable |
disable ]
[no] openflow instance { instance-name | aggregate }
enable
```

The `no` form of the command deletes **all** OpenFlow configurations for the instance.

`instance-name` Creates an OpenFlow instance.

Instance names can have a maximum length of 32 case-insensitive alphanumeric characters, numerals, and underscore.

`aggregate`	Creates an OpenFlow instance that includes all VLANs except the management VLAN and the OpenFlow controller VLANs. See “Aggregation mode” (page 9) for details on the use of this parameter.
`enable`	Enables the named OpenFlow instance or aggregate.
`disable`	Disables the named OpenFlow instance or aggregate.

OpenFlow instance mode

OpenFlow can work either in *`active`* or *`passive`* mode.

Active mode	New packets of a flow that the switch is not aware of are sent to the OpenFlow controller.
Passive mode	There is one-way communication from the OpenFlow controller to the switch. Packets that do not match any flow in the flow table on the switch are not sent to the controller. Such packets of new flows are handled normally by the switch.

NOTE: This option is applicable only for an OpenFlow version 1.0 instance.

This command sets operation mode for an OpenFlow instance.

Syntax

```
openflow instance { instance-name | aggregate }
mode { active | passive }
```

`instance` *`instance-name`*	Sets the mode for the named instance.
`aggregate`	Sets the mode for the aggregate instance.
`active`	New flows are redirected to the controller for the instance.
`passive`	New flows are not sent to the controller for the instance.

Default: active

Configure OpenFlow instance members

- Only one VLAN can be added as a member of an OpenFlow instance in virtualization mode.
- The same VLAN cannot be added as a member of multiple OpenFlow instances.
- The management VLAN cannot be added to an OpenFlow instance as a member VLAN.
- A Controller VLAN cannot be added to an OpenFlow instance as a member VLAN.

Syntax

```
[no] openflow instance instance-name
member vlan vlan-id
```

`instance-name`	Add a member to this OpenFlow instance.
`vlan` *`vlan-id`*	Adds the VLAN to the named OpenFlow instance.

Flow location

This command sets the location of flows for an instance or the aggregate. In hardware-only mode, flows are programmed only in hardware. The flows are located in hardware and software by default.

Syntax

[no] openflow instance { *instance-name* | aggregate } flow-location hardware-only

instance-name	Sets flow location for the named instance.
aggregate	Sets flow location for the aggregate instance.
hardware-only	Sets the location of flows to hardware only.

Default: Software and hardware.

NOTE: An error is returned to the controller if the flow cannot be added in hardware and the flow-location is set as hardware-only.

Communicating port status to the controller

OpenFlow provides the ability to program flows for ports which are not up yet. The OpenFlow switch communicates port state notification to the controller as part of OFPT_PORT_STATUS message. This allows the controller to pre-provision flows in the switch referring ports that may be down. The post status messages are:

- OFPPS_LIVE – Physical link present
- OFPPS_LINK_DOWN – No physical link present
- OFPPS_BLOCKED – Port is blocked

Example

```
HP-Stack-3800(openflow)# show vlan 3
Status and Counters - VLAN Information - VLAN 3
VLAN ID : 3
Name    : VLAN3
Status  : Port-based
Voice   : No
Jumbo   : No

Port Information  Mode         Unknown VLAN  Status
----------------  --------   ------------   ----------
1/1               Untagged    Learn         Up
1/2               Untagged    Learn         Up
1/4               Untagged    Learn         Down
1/5               Untagged    Learn         Down

openflow@openflow-ubuntu-02:~$ dpctl tcp:20.0.0.1:6633 port-desc
SENDING:
stat_req{type="port-desc", flags="0x0"}

RECEIVED:
stat_repl {type="port-desc", flags="0x0"

{no="4", hw_addr="08:2e:5f:69:6e:7c", name="1/4", config="0x0"
, state="0x1", curr="0x0", adv="0x0", supp="0x0", peer="0x0",
curr_spd="0kbps", max_spd="0kbps"},

{no="2", hw_addr="08:2e:5f:69:6e:7e", name="1/2", config="0x0",
state="0x4", curr="0x220", adv="0x0", supp="0x22f",
peer="0x0", curr_spd="3567587328kbps", max_spd="3567587328kbps"},

{no="5", hw_addr="08:2e:5f:69:6e:7b", name="1/5", config="0x0",
state="0x1", curr="0x0", adv="0x0", supp="0x0", peer="0x0",
curr_spd="0kbps", max_spd="0kbps"},

{no="local", hw_addr="08:2e:5f:69:6e:65", name="local",
```

```
config="0x0", state="0x0", curr="0x0", adv="0x0", supp="0x0",
peer="0x0", curr_spd="0kbps", max_spd="0kbps"},

{no="1", hw_addr="08:2e:5f:69:6e:7f", name="1/1", ="0x0",
state="0x4", curr="0x220", adv="0x0", supp="0x22f", peer="0x0",
curr_spd="3567587328kbps", max_spd="3567587328kbps"}}}
```

Configuring listener ports

Configures an OpenFlow port to listen for incoming connections from an OpenFlow controller.

Syntax

```
[no] openflow instance { instance-name | aggregate }
listen-port [tcp-port] [oobm]
```

instance-name	Sets the `listen-port` for the named instance.
`aggregate`	Sets the `listen-port` for the aggregate instance.
tcp-port	Specify the port to listen on. Default: Port number 6633 Range: Port number 1024 - 65536
`oobm`	Configure to listen through the out-of-band management (OOBM) port. This is only applicable for switches that have a separate OOBM port.

Configuring a controller

A controller is identified by its IP address and a connection port. Each OpenFlow instance can have up to 3 controllers. OpenFlow controllers can be added or deleted using this command.

Syntax

```
openflow controller-id <id> [ip <ip-address>] [port <tcp-port>]
controller-interface { vlan <vlan-id> | oobm }
[no] openflow controller-id <id>
```

id	OpenFlow controller identification number. The `no` removes the identified controller, if the controller is not in use by any OpenFlow instances. Range: 1 – 128
ip-address	OpenFlow controller IP address.
tcp-port	Optional: Specify the port through which to connect to a controller. Default: port number 6633 Range: 1024 – 65535
`controller-interface`	The `no` form of the command with this parameter deletes the OpenFlow controller connection.
vlan-id	Connect to the OpenFlow controller through the identified VLAN. **NOTE:** A VLAN that is a member of an OpenFlow instance cannot be added as an OpenFlow controller interface.

`oobm` Connect to the OpenFlow controller through the OOBM interface. Only applicable for switches that have a separate out-of-band management (OOBM) port.

Associate OpenFlow instance with OpenFlow controller

Once the OpenFlow controller is set up, each instance must be associated to a controller.

Syntax

`[no] openflow instance { instance-name | aggregate } controller-id controller-ID`

Up to three controllers can be specified per OpenFlow instance.

The `[no]` removes the identified controllers.

`instance-name` Sets controller for the named instance.

`aggregate` Sets controller for the aggregate instance.

`controller-ID` OpenFlow controller ID to be associated with the instance; up to 3 controllers per instance.

Example-Associating an OpenFlow instance with multiple controllers

To associate controllers 1, 5, and 100 to instance “test”, use the following commands:

```
HPswitch(config)# openflow instance test controller-id 1
#openflow instance test controller-id 5
#openflow instance test controller-id 100
```

NOTE: When an OpenFlow controller is associated with an OpenFlow instance it cannot be deleted.

Securing the connection between an OpenFlow instance and the controller

Syntax

`[no] controller-id controller-id secure`

`secure` Initiates a TLS connection with the controller (TLS version 1.0 or greater.)

This command:

- Secures the instance controller main connection. This option is available for OpenFlow version1.0 as well as OpenFlow version 1.3.
- Supports CA signed certificates. For CA signed certificates, same ROOT certificate is used to sign both controller and switch certificate.
- Supports mutual authentication.

Example

```
HP-3500yl-48G-PoEP(of-inst-t1)# show openflow instance t1
Configured OF Version    : 1.3
Negotiated OF Version    : 1.3
Instance Name            : t1
Admin. Status            : Enabled
Member List              : VLAN 3
Listen Port              : None
```

```
Oper. Status             : Up
Oper. Status Reason      : NA
Datapath ID              : 0003b499ba86bf80
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : NA
No. of Sw Flow Tables    : 1
Egress Only Ports        : None
Table Model              : Policy Engine and Software

Controller Id  Connection Status  Connection State Secure Role
-------------- ----------------- - --------------- - ------ -----
1              Connected          Active            Yes    Equal
```

Configuring auxiliary connections

Syntax

`openflow # auxiliary-connection` *index* `port` *port-number* `type tcp|udp`

Creates an auxiliary connection with a unique index which is later associated with the instance controller main connection. Auxiliary connection uses the same source IP address and the datapath ID as the main connection. The main connection auxiliary ID is set to zero, while the auxiliary connection ID is set to 1. Only one auxiliary connection is supported per main connection and transport protocol options for auxiliary connections can be either TCP or UDP.

The packets supported on an auxiliary channel are:

- OFPT_HELLO
- OFPT_ERROR
- OFPT_ECHO_REQUEST/ REPLY
- OFPT_FEATURES_REQUEST/REPLY
- OFPT_PACKET_IN
- OFPT_PACKET_OUT

The main use of an auxiliary connection is for transactions related to message of type: OFPT_PACKET_IN/OFPT_PACKET_OUT.

Options

index Unique identifier for an auxiliary connection.

port Protocol port on which the controller can be reached.

type Type of transport protocol to be used: TCP or UDP.

`[no]` Removes the auxiliary connection.

NOTE: Auxiliary connections are terminated when the main connection goes down or is closed by the user or when the OpenFlow instance/openflow is disabled or OpenFlow is globally disabled.

TLS is not supported for Auxiliary connections.

Example

```
HP-Stack-3800(openflow)# auxiliary-connection 1 port 6633 type tcp
HP-Stack-3800(openflow)# inst t1
HP-Stack-3800(of-inst-t1)# controller-id 1 auxiliary-connection 1

HP-E5406zl(config)# show openflow instance t1
Configured OF Version    : 1.3
Negotiated OF Version    : NA
Instance Name            : t1
Admin. Status            : Enabled
Member List              : VLAN 2
Listen Port              : 6633
Oper. Status             : Down
Oper. Status Reason      : NA
Datapath ID              : 0000002320e877fe
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : NA
No. of Sw Flow Tables    : 1
Egress Only Ports        : None
Table Model              : Single Table

Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1             Disconnected      Void             No     Equal

 Auxiliary            Auxiliary               Auxiliary
 Controller Id Conn. index Auxiliary ID Conn. Status Conn. State Type
 ------------- ----------- ------------ ------------ ----------- ----
1              1           1            Disconnected  Void        TCP


#HP-8206zl# show run
openflow
 controller-id 1 ip 20.0.0.2 controller-interface vlan 1
  auxiliary-connection 1 port 6633 type tcp
  instance "t1"
   listen-port
  member vlan2
  controller-id 1 auxiliary-connection 1
  version 1.3
  enable
   exit
 enable
  exit
```

Associating the auxiliary connection index with an OpenFlow instance

Syntax

`openflow instance` *`instance-name`* `auxiliary connection` *`auxiliary-connection-index`*

Range for the auxiliary connection index: 1–128

Only one auxiliary connection is supported per main controller connection.

Configuring number of software flow tables per instance

Syntax

`openflow instance` *`instance-name`* `software-flow-table` *`number-of-software-tables`*

Configures the number of software flow tables required for an instance.

Default: 1, Range: 1–4

This is applicable only for an OpenFlow version 1.3 instance.

OpenFlow instance connection interruption mode

Use this to set behavior when an OpenFlow instance on the switch loses connection with the controller.

Syntax

[`no`] `openflow instance` [*`instance-name`*] `connection-interruption-mode` { `fail-secure` | `fail-standalone` }

`fail-secure`	If this OpenFlow instance on the switch loses connection with all controllers, packets and messages intended for controllers are dropped. Flows continue to expire according to their time-outs. Default: `fail-secure`
`fail-standalone`	If this OpenFlow instance on the switch loses connection with all controllers, packets of new flows are handled by the legacy switching and routing functions. Existing flows of this OpenFlow instance are removed.

Setting maximum backoff interval for an instance

You can specify the maximum interval between two consecutive attempts to connect to a controller by an OpenFlow instance. The interval between two consecutive attempts increases exponentially until it reaches the specified value. All subsequent attempts use the specified value.

Syntax

`openflow instance` { *`instance-name`* | `aggregate` } `max-backoff-interval` *`seconds`*

`instance-name`	Sets the backoff interval for the named instance.
`aggregate`	Sets the backoff interval for the aggregate instance.
`seconds`	Default: 60 seconds; Range: 1 — 3600 seconds

Configuring IP Control Table Mode

Depreciated syntax. See the command `[no] pipeline-model standard-match|ip-control|custom`.

Syntax

`openflow [no] ip-control-table-mode`

Includes IP control table in the OpenFlow packet processing pipeline.

Configure OpenFlow controller ports

An OpenFlow controller is configured globally under OpenFlow context and associated with an instance under instance context (see “Entering OpenFlow instance context” (page 16) for more information). OpenFlow controller traffic cannot be “in-band” or transit on a VLAN managed by OpenFlow. It must transit on a VLAN not managed by OpenFlow.

OpenFlow controller traffic and OpenFlow traffic can transit on the same port, as long as they use different VLANs.

The VLAN chosen for OpenFlow controller traffic depends entirely on the IP address of the controller, and no specific configuration is needed. Thus the switch must have a proper IP configuration, and the controller address must be part of a subnet that is not on an OpenFlow VLAN.

For information on how to either manually assign an IP address to the switch or set it up to perform DHCP queries, see the ‘Configuring IP Addressing’ chapter in the *Basic Operation Guide* for your HP switch.

Each OpenFlow instance can be controlled by up to three OpenFlow controllers and each generates OpenFlow commands and data flows between an OpenFlow switch and the controller.

Controller roles

By operating in different modes, controllers can synchronize handoffs in a scenario where multiple controllers are connected to the switch. Per the OpenFlow specification 1.3.1, a Controller can operate in one of the following roles:

- Equal
- Master
- Slave

Equal This is the default role for a controller. The controller has full access to the switch and is equal to other controllers in the same role receiving all asynchronous messages from the switch (such as packet-in, flow-removed, etc.) Controller-to-switch commands are sent and modified within this role.

Slave A Slave controller has read-only access to the switch. The controller cannot receive switch asynchronous messages except for Port-status messages. The controller is denied execution of the controller-to-switch commands: OFPT_PACKET_OUT, OFPT_FLOW_MOD, OFPT_GROUP_MOD, OFPT_PORT_MOD and OFPT_TABLE_MOD.

Master The Master controller has full read-write access to the switch. Only one controller can be the Master at a given time. When a controller’s role is changed to Master, the switch will automatically change all other controllers, that it connects to, to a Slave role.

Syntax

To know the roles of controllers that a switch is connected to, use the following command:

```
show openflow instance instance-name
```

Example

```
HP-3500yl-48G-PoEP(of-inst-t1)# show openflow instance t1
Configured OF Version       : 1.3
Negotiated OF Version       : 1.3
Instance Name               : t1
Admin. Status               : Enabled
Member List                 : VLAN 3
Listen Port                 : None
Oper. Status                : Up
Oper. Status Reason         : NA
Datapath ID                 : 0003b499ba86bf80
Mode                        : Active
Flow Location               : Hardware and Software
No. of Hw Flows             : 0
No. of Sw Flows             : 0
Hw. Rate Limit              : 0 kbps
Sw. Rate Limit              : 100 pps
Conn. Interrupt Mode        : Fail-Secure
Maximum Backoff Interval    : 60 seconds
Probe Interval              : 10 seconds
Hw. Table Miss Count        : NA
No. of Sw Flow Tables       : 1
Egress Only Ports           : None
Table Model                 : Policy Engine and Software

Controller Id Connection Status Connection State  Secure  Role
------------- ----------------- ----------------  ------  ------
1                 Connected           Active              No
    Slave
2                 Connected           Active              No
    Master
```

Controller role change

The following messages are related to controller role change:

OFPT_ROLE_REQUEST	Message from controller to the switch to change or query its role.
OFPT_ROLE_REPLY	Message sent in response to the OFPT_ROLE_REQUEST, returning the current role of the controller.
OFPT_SET_ASYNC	A controller, through this message can configure what asynchronous message notifications it wants to receive.
OFPT_GET_ASYNC	Controller uses this message to retrieve the asynchronous configuration set using the OFPT_SET_ASYNC message.

NOTE: Whenever a connection is established between the switch and the controller, each controller starts in the role, OFPCR_ROLE_EQUAL. The controller can query and change its role if required.

Port modification

Port modification is used to change the characteristics of a port in an OpenFlow instance on the switch via the controller. The controller sends an OFP_PORT_MOD message to the switch that can change the characteristics of a specific port.

The following command checks the state of the port configuration for all ports of an instance.

Syntax

```
show openflow instance instance-name port-statistics
```

Example

```
HP-Stack-3800(of-inst-t1)# show openflowinstance t1 port-statistics
Number of Ports :1
Port 1/1        : Up
Status
Admin. Status     : Enabled        Flood    : Enabled
Receive           : Enabled        Forward  : Enabled
Packet_in         : Disabled
Statistics
  Collisions     : 0
  Rx Packets     : 0             TxPackets : 47
  Rx Bytes       : 0             TxBytes   : 10718
  Rx Dropped     : 0             TxDropped : 0
  Rx Errors      : 0             TxErrors  : 0
   Frame Errors    : 0
   CRC Errors     : 0
   Overrun Errors : 0
```

Example-OpenFlow version 1.0

```
Wireshark Capture of a sample Port-Mod message for a 1.0 instance

OpenFlow Protocol
  Header
   Version: 0x01
   Type: Port Mod (CSM) (15)
   Length: 32
   Transaction ID: 4
  Port Modification
   Port #: 5
    MAC Address: HewlettP_02:2c:bb (84:34:97:02:2c:bb)
Port ConfigFlags
.... .... .... .... .... .... .... ...0 = Port is administratively down: No (0)
.... .... .... .... .... .... .... ..0. = Disable 802.1D spanning tree on port: No (0)
.... .... .... .... .... .... .... .0.. = Drop non-802.1D packets received on port: No (0)
.... .... .... .... .... .... .... 0... = Drop received 802.1D STP packets: No (0)
.... .... .... .... .... .... .... ...1 .... = Do not include this port when flooding: Yes (1)
.... .... .... .... .... .... ..0. .... = Drop packets forwarded to port: No (0)
.... .... .... .... .... .... .0.. .... = Do not send packet-in msgs for port: No (0)
Port Config Mask
.... .... .... .... .... .... .... ...0 = Port is administratively down: No (0)
.... .... .... .... .... .... .... ..0. = Disable 802.1D spanning tree on port: No (0)
.... .... .... .... .... .... .... .0.. = Drop non-802.1D packets received on port: No (0)
.... .... .... .... .... .... .... 0... = Drop received 802.1D STP packets: No (0)
.... .... .... .... .... .... ...1 .... = Do not include this port when flooding: Yes (1)
.... .... .... .... .... .... ..0. .... = Drop packets forwarded to port: No (0)
.... .... .... .... .... .... .0.. .... = Do not send packet-in msgs for port: No (0)
Port Advertise Flags
.... .... .... .... .... .... .... ...0 = 10 Mb half-duplex rate support: No (0)
.... .... .... .... .... .... .... ..0. = 10 Mb full-duplex rate support: No (0)
.... .... .... .... .... .... .... .0.. = 100 Mb half-duplex rate support: No (0)
.... .... .... .... .... .... .... 0... = 100 Mb full-duplex rate support: No (0)
... .... .... .... .... .... ...0 .... = 1 Gb half-duplex rate support: No (0)
.... .... .... .... .... .... ..0. .... = 1 Gb full-duplex rate support: No (0)
.... .... .... .... .... .... .0.. .... = 10 Gb full-duplex rate support: No (0)
.... .... .... .... .... .... 0... .... = Copper medium support: No (0)
.... .... .... .... .... ...0 .... .... = Fiber medium support: No (0)
.... .... .... .... .... ..0. .... .... = Auto-negotiation support: No (0)
 .... .... .... .... .... .0.. .... .... = Pause support: No (0)
.... .... .... .... .... 0... .... .... = Asymmetric pause support: No (0)
Pad: 0
Pad: 0
Pad: 0
Pad: 0
```

Example-OpenFlow version 1.3

```
Wireshark Capture of a sample Port-Mod message for a 1.3 instance
OpenFlow Protocol
  Header
```

```
   Version: 0x04
   Type: Port Mod (CSM) (16)
    Length: 40
   Transaction ID: 4043243760
   Port Modification
   Port #: 2
   Pad: 0
    Pad: 0
    Pad: 0
    Pad: 0
  MAC Address: HewlettP_02:2c:be (84:34:97:02:2c:be)
    Pad: 0
   Pad: 0
   Port ConfigFlags
.... .... .... .... .... .... .... ...0 = Port is administratively down: No (0)
.... .... .... .... .... .... .... ..0. = Disable 802.1D spanning tree on port: No (0)
.... .... .... .... .... .... .... .0.. = Drop non-802.1D packets received on port: No (0)
.... .... .... .... .... .... .... 0... = Drop received 802.1D STP packets: No (0)
.... .... .... .... .... .... ...0 .... = Do not include this port when flooding: No (0)
.... .... .... .... .... .... ..0. .... = Drop packets forwarded to port: No (0)
.... .... .... .... .... .... .1.. .... = Do not send packet-in msgs for port: Yes (1)
   Port Config Mask
.... .... .... .... .... .... .... ...0 = Port is administratively down: No (0)
.... .... .... .... .... .... .... ..0. = Disable 802.1D spanning tree on port: No (0)
.... .... .... .... .... .... .... .0.. = Drop non-802.1D packets received on port: No (0)
.... .... .... .... .... .... .... 0... = Drop received 802.1D STP packets: No (0)
.... .... .... .... .... .... ...0 .... = Do not include this port when flooding: No (0)
.... .... .... .... .... .... ..0. .... = Drop packets forwarded to port: No (0)
.... .... .... .... .... .... .1.. .... = Do not send packet-in msgs for port: Yes (1)
  Port Advertise Flags
.... .... .... .... .... .... .... ...0 = 10 Mb half-duplex rate support: No (0)
.... .... .... .... .... .... .... ..0. = 10 Mb full-duplex rate support: No (0)
.... .... .... .... .... .... .... .0.. = 100 Mb half-duplex rate support: No (0)
.... .... .... .... .... .... .... 0... = 100 Mb full-duplex rate support: No (0)
.... .... .... .... .... .... ...0 .... = 1 Gb half-duplex rate support: No (0)
.... .... .... .... .... .... ..0. .... = 1 Gb full-duplex rate support: No (0)
.... .... .... .... .... .... .0.. .... = 10 Gb full-duplex rate support: No (0)
.... .... .... .... .... .... 0... .... = Copper medium support: No (0)
.... .... .... .... .... ...0 .... .... = Fiber medium support: No (0)
.... .... .... .... .... ..0. .... .... = Auto-negotiation support: No (0)
.... .... .... .... .... .0.. .... .... = Pause support: No (0)
.... .... .... .... .... 0... .... .... = Asymmetric pause support: No (0)
   Pad: 0
   Pad: 0
  Pad: 0
  Pad: 0
```

Example

Send a Port-Mod command to the switch using dpctl, a controller utility.

```
root@openflow-ubuntu-10:/home/openflow# dpctltcp:10.20.30.50:6633 port-desc

... {no="6", hw_addr="00:1b:3f:cf:76:fa", name="A6", config="0x0", state="0x1",
curr="0x0", adv="0x0", supp="0x0", peer="0x0", curr_spd="100000000kbps",
max_spd="100000000kbps"} ...

root@openflow-ubuntu-10:/home/openflow# dpctltcp:10.20.30.50:6633 port-mod
port=6,addr=00:1b:3f:cf:76:fa,conf=0x40,mask=0x40

SENDING:
port_mod{port="6", hwaddr="00:1b:3f:cf:76:fa", config="0x00000040",
mask="0x40", adv="0x0"}
OK

root@openflow-ubuntu-10:/home/openflow# dpctltcp:10.20.30.50:6633 port-desc
... {no="6", hw_addr="00:1b:3f:cf:76:fa", name="A6", config="0x40",
state="0x1", curr="0x0", adv="0x0", supp="0x0", peer="0x0",
curr_spd="100000000kbps", max_spd="100000000kbps"} ...
```

Port modification and OpenFlow versions

OFP_PORT_CONFIG, OFPPC_NO_FLOOD and OFPPC_NO_PACKET_IN are supported by an OpenFlow 1.0 instance on the switch.

OFP_NO_FLOOD and OFPPC_NO_PACKET_IN are supported by an OpenFlow v1.3 instance on the switch.

NOTE: If a port is not exclusive to the Openflow Member VLAN, a Port Modification message from the controller will result in an error returned to the controller.

Configuring egress only ports

This CLI command enables or disables support for advertising egress-only ports to the controller. Ports that are members of non-OpenFlow VLANs are egress-only ports. A controller can add a flow with an egress-only port as an output port to allow traffic to be forwarded from an OpenFlow VLAN to a non-OpenFlow VLAN. All instance member ports and egress-only ports are exposed as instance ports to the controller.

Syntax

```
openflow egress-only-ports
```

egress-only-ports — Enable or disable support for advertising egress-only ports to the controller.

Ports that are members of non-OpenFlow VLANs are egress-only ports. A controller can add a flow with an egress-only port as an output port to enable traffic to be forwarded from an OpenFlow VLAN to a non-OpenFlow VLAN.

NOTE: Egress-only ports cannot be used as an “in-port” in any flow by a controller. If this is attempted, the flow addition will fail and an error message will be returned to the controller.

Example

```
Openflow # egress-only-ports
Configured OF Version   : 1.0
Negotiated OF Version   : 1.0
Instance Name           : test
Admin. Status           : Enabled
Member List             : VLAN 3
Listen Port             : None
Oper. Status            : Up\
Oper. Status Reason     : NA
DatapathID              : 00032c4138c98500
Mode                    : Active
Flow Location           : Hardware and Software
No. of Hw Flows         : 0
No. of Sw Flows         : 0
Hw. Rate Limit          : 0 kbps
Sw. Rate Limit          : 100 pps
Conn. Interrupt Mode    : Fail-Secure
 Maximum BackoffInterval : 60 seconds
Probe Interval          : 10 seconds
Hw. Table Miss Count    : 0
No. of Sw Flow Tables   : NA
Egress Only Ports       : A1,A3-A24,F1-F22

Table Model: Single Table

Controller id  Connection Status Connection State Secure  Role
-------------- ----------------- ---------------- ------  ------
1              Disconnected      Backoff          No      Equal
```

NOTE: When the Egress-Only Ports option is enabled for OpenFlow on the switch, the Port-Mod message for an egress-only port will result in an error.

Software and hardware rate limiting

You can specify resource limits used by an OpenFlow instance. Each OpenFlow instance has completely independent rate-limiters that can be set separately.

Syntax

```
openflow instance { instance-name | aggregate }
limit { hardware-rate kbps | software-rate pps }
```

instance-name Set software and hardware rate limiting for the named instance.

aggregate Set software and hardware rate limiting for the aggregate instance.

kbps Limit the bandwidth that can be utilized by an OpenFlow instance.

Default: 0 kbpsRange 0 — 10,000,000 kbps

pps Configure the OpenFlow instance packet rate limit.

Limits the number of packets per second per module that this instance can send to the software path.

Default: 100 ppsRange: 1 — 10,000 pps

NOTE: Increasing the software rate limit increases CPU consumption and may impact system performance.

If the software rate limit is specified beyond 1000 pps, the warning listed below will be displayed:

```
Increasing the software rate limit would increase CPU
consumption and may impact the system performance.
```

Limiting the usage of hardware resources

Syntax

```
openFlow limit policy-engine-usage | ip-ctrl-table-usage |
multiport-filter-usage max-percentage
```

policy-engine-usage Maximum percentage of policy engine resources used by OpenFlow.

ip-ctrl-table-usage Maximum percentage of IP control table resources used by OpenFlow.

multiport-filter-usage Maximum percentage of the multiport-filter resources used by OpenFlow.

You can limit the OpenFlow usage of policy engine resources, ip control table and multiport filters so that other functions that use the same resources are not impacted severely.

The limit can only be set when OpenFlow is disabled globally.

Max-Percent Specifying 0% allocates no resources for OpenFlow.

By default, the OpenFlow policy engine resource usage is set at 50% to avoid oversubscribing resources and impacting performance. In addition to OpenFlow, the policy engine resource can be used by Access Control Lists, Quality of

Service, Identity Driven Management, Virus Throttling, Mirroring, Policy Based Routing, and other features.

NOTE: The maximum percentage is not a guaranteed percentage but a maximum allowed limit.

To increase the number of flows beyond the default 50% setting, use the above OpenFlow limit policy-engine-usage command. If all policy engine resources are in use, OpenFlow rules will no longer be added in hardware and the switch will deny attempts to configure ACLs with the CLI. See “Monitoring Resources” in the latest *Management and Configuration Guide* for your switch.

Default: 50%; Range: 0 — 100%

NOTE: Resource usage can only be set when OpenFlow is disabled.

Example

```
openflow# limit multiport-filter-usage [1-100]
0-100:  Maximum percentage of Multiport filters used by OpenFlow.

HP-3500yl-24G-PoEP# show openflow multiport-filter-limit
Total Multiport Filters: 2037
                 Filters       Filters        Filters
Features       Allocated    Used            Free
-------------- ---------- -----------  -----------
OpenFlow       1024            0                1024
```

Hardware statistics refresh rate

Syntax

`openflow` *`instance-name`* `hardware statistics|refresh rate policy-engine-table` *`seconds`*

Refresh rate for policy engine table statistics.

Default: 0–3600

Backing up your configuration (optional)

Dual management module in E8200 platforms is supported. Flow configuration is synchronized across management modules and flow table preserved during switchover.

See ‘Chassis Redundancy’ in the *Management and Configuration Guide* for your switch.

Configuring VLANs

For information on configuring and verifying VLANs, see the *Advanced Traffic Management Guide* for your switch.

Configuring and verifying routing

For information on configuring and verifying routing, see the *Multicast and Routing Guide* for your switch.

Configuring physical and logical ports

For information on configuring and verifying ports, see the ‘Port Status and Configuration’ chapter in the *Management and Configuration Guide* for your switch.

Pipeline configuration commands

Syntax

[no]pipeline-model standard-match|ip-control|custom

Configure an OpenFlow instance pipeline model. By default, the instance is configured to use the standard-match pipeline model.

standard-match	Configure a standard-match pipeline model. The standard-match pipeline model enables an instance to advertise its policy-engine and software tables.
ip-control	Configure an ip-control pipeline model. The ip-control pipeline model enables an OpenFlow version 1.3 instance to advertise its IP control table along with policy-engine and software tables.
custom	Configure a custom pipeline model. The custom pipeline model enables an OpenFlow controller to customize an Openflow pipeline model for OpenFlow version 1.3 instance.

Syntax

openflow instance INSTANCE-NAME

An instance without “pipeline-model” configured defaults to standard-match but will change to ip-control mode when ip-control-mode is globally enabled. An instance with “pipeline-model” configured as standard-match will not change to ip-control mode when ip-control-mode is globally enabled.

connection-interru.	Set the type of behavior when the switch loses connection with the controller.
controller-id	Add controllers for an OpenFlow instance.
disable	Disable the current OpenFlow instance.
enable	Enable the current OpenFlow instance.
flow-location	Set the location of the flows used by this instance.
limit	Set limit on resource usage by an OpenFlow instance.
listen-port	Specify TCP the port on which the OpenFlow agent of the switch waits (listens) for incoming connections from a OpenFlow controller.
max-backoff-interval	Specify the maximum interval between two consecutive attempts to connect to a controller.
member	Add members to this OpenFlow instance.
mode	Set the operation mode of the OpenFlow instance.
probe-interval	The probe interval is the time between two consecutive probes sent from an instance to the controller.
software-flow-table	Specify the number of software flow tables required per instance.
version	OpenFlow protocol version supported for the specific instance.
pipeline-model	Configure an OpenFlow instance pipeline model.
standard-match	Configure a standard-match pipeline model.

ip-control	Configure an ip-control pipeline model.
custom	Configure a custom pipeline model.

Validation rules

Validation	Error/Warning/Prompt
Custom pipeline model is available only in V3-only mode.	Custom pipeline model cannot be set on v1/v2 modules.
Version can only be “1.3 only” if an instance has to be enabled in custom match mode. HP does not support “1.0” or “1.3”, in custom mode – only “1.3 only” is required.	Instance version should be “1.3 only” if pipeline-model is custom.

Openflow MAC group

MAC Group Tables allows the controller to apply the same policy to a set of users, differentiated by the source MAC address, using a single rule in the policy table. This is achieved by exposing the MAC CAM as a separate table to controllers and allows controllers to create MAC groups.

OpenFlow pipeline

MAC group tables can be enabled for an OpenFlow instance in “standard match mode” or “ip control mode”. By default, both **source mac group** table and **destination mac group** tables are disabled. These tables can be enabled in the pipeline by using the commands `src-mac-grp-table` or `dest-mac-grp-table`. The figures below depict the various combinations of OpenFlow pipelines that an instance can have.

Figure 5 Standard match mode default pipeline



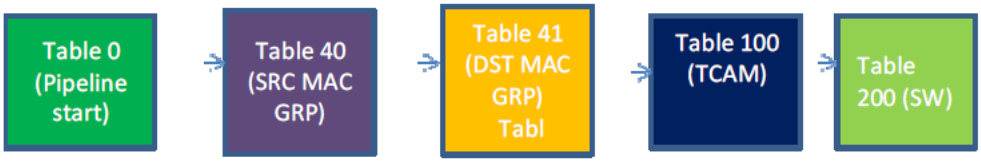
Figure 6 Standard match SRC enabled pipeline



Figure 7 Standard match DST enabled pipeline



Figure 8 Standard match SRC and DST enabled pipeline



IP control table pipeline

A single consolidated policy table combines “IP Match Policy Table”, “IP Miss Policy Table” and “Non-IP Policy table”. “Policy table” in IP control table mode allows the controller to match on L3 match, L3 miss and L3 ignore. OpenFlow controller must program rules into policy table with metadata to achieve functionality. Table 3 illustrates the values of metadata and metadata mask that needs to be programmed.

Figure 9 IP control destination MAC enabled pipeline

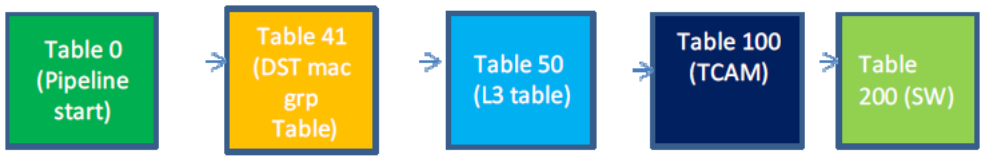


Figure 10 IP control source MAC enabled pipeline



Figure 11 IP control table default



Metadata

The controller must program rules with match on metadata to achieve functionality.

The following table illustrates the values of metadata and metadata mask with which these functionalities can be achieved.

Table 3 Metadata

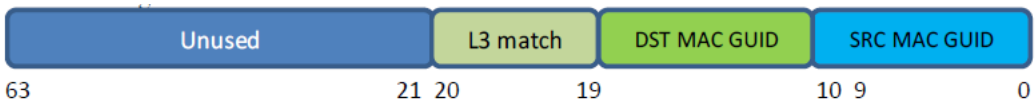
	Metadata	Metadata_mask
L3 match	1	1
L3 miss	0	1
L3 ignore	0	0
Non-IP		

OpenFlow provides support for metadata, which is a maskable register value that is used to carry information from one table to the next.

Example 1 OpenFlow metadata

For example `OFPXMT_OFB_METADATA` is part of `oxm_ofb_match_fields` and is a 64 bit field. It is used to pass information between lookups across multiple tables. This value can be arbitrarily masked. Out of 64 bits, current release is using 21 bits and the following table illustrates the interpretation of these bits.

Figure 12 OpenFlow metadata



- `SRC MAC GRP` – 10 bits which identifies the Source Mac Group ID
- `DST MAC GRP` – 10 bits which identifies the destination Mac Group ID
- `L3 match` – 1 bit which is used to identify L3 match/miss in case of ip control table mode.

The following table shows the values of Metadata_match and metadata_write bits advertised for different table

Table 4 Bits advertised

Table #	Metadata_match	Metadata_write
0	0	0
40	0	0x3FF (Bits 0 to 19)(Bits 0 to 9 are used to write the src GUID for MAC)
41	0	0xFFC00 (Bits 10 to 19) (Bits 0 to 9 are used to write the dst GUID for MAC)
50	0	0x100000 (Bit 20)
100	0x01FFFFF (Bits 0 to 20)	0
200	0	0

NOTE:

- Rules on the policy table must match on metadata which in turn is mapped to a MAC-group (source/destination MAC).
- The policy table cannot match on a source MAC and destination MAC address separately when MAC group tables are part of the pipeline.
- In L3 tables, rules can be added with instructions `WRITE_METADATA/MASK` and `GOTO`.
- On the policy table, the L3 match, L3 miss is interpreted by the metadata, metadata_mask specified in the rule.

Command to configure source MAC group table on an instance

Syntax

From within an OpenFlow instance:
[no]`openflow ins` *`instance name`* `src-mac-grp-table`

Enable the source MAC group table in the OpenFlow pipeline.

Options

`src-mac-grp-table`	Enable the source MAC group table in the OpenFlow pipeline.
`connection-interru`	Set the type of behavior when the switch loses connection with the controller.
`controller-id`	Add controllers for an OpenFlow instance.
`datapath-desc`	Specify a description for the data path
`dest-mac-grp-table`	Enable the destination MAC group table in the OpenFlow pipeline.
`disable`	Disable the current OpenFlow instance.
`enable`	Enable the current OpenFlow instance.
`flow-location`	Specify the location of the flows that are used by this instance.
`limit`	Set the limit on resource usage by an OpenFlow instance.
`listen-port`	Specify the TCP port on which the OpenFlow agent of the switch waits (listens) for incoming connections from an OpenFlow controller.
`max-backoff-interval`	Specify the maximum interval between two consecutive attempts to connect to a controller.
`member`	Add member VLANs to this OpenFlow instance.
`mode`	Set the operation mode of the OpenFlow instance.
`pipeline-model`	Configure an OpenFlow instance pipeline model.
`probe-interval`	The probe interval is the time between two consecutive probes sent from an instance to the controller.
`software-flow-table`	Specify the number of software flow tables required per instance.
`version`	Specify the OpenFlow protocol version supported for the specific instance.

Validation rules

Validation	Error/Warning/Prompt
Source MAC group table can be enabled on only one instance.	The source MAC group table cannot be enabled on multiple instances.
Source MAC group table is supported only in standard match mode/ip-control-table mode.	The source MAC group table is not supported on custom-pipeline mode.
In ip-control-table mode, both source MAC groups and destination MAC groups cannot be configured.	The source MAC group table cannot be enabled when the destination MAC group table is enabled in IP control pipeline mode.
When enabling the mac group table, the oper statuses of all other instances have to be down.	All the instances must be disabled before enabling the source MAC group table.
Flow table number modification needs to be blocked when MAC group table is enabled.	Flow table number modification is not allowed when a MAC group table is enabled.

Validation	Error/Warning/Prompt
MAC group feature is not available in V1 compatibility mode.	The source MAC group table is not supported when the switch is in V1 module compatible mode.
If an instance is standard-match mode source and destination tables can be enabled. When both are enabled pipeline-model cannot be changed to ip-control.	Pipeline-model cannot be changed to ip-control if both source and destination MAC group tables are enabled.
Source and destination MAC group tables cannot be enabled when table-numbers are customized by user MAC group tables cannot be enabled.	The source MAC group table cannot be enabled. The flow table numbers need to be reset to their default values.
When MAC group tables are configured instance pipeline-model cannot be changed to custom.	Pipeline-model cannot be changed to custom when a MAC group table is enabled.

Destination MAC group table on an instance

Syntax

[no]openflow instance *instance name* dest-mac-grp-table

Enable the destination MAC group table in the OpenFlow pipeline.

connection-interru	Set the type of behavior when the switch loses connection with the controller.
controller-id	Add controllers for an OpenFlow instance.
datapath-desc	Specify a description for the data path.
dest-mac-grp-table	Enable the destination MAC group table in the OpenFlow pipeline.
disable	Disable the current OpenFlow instance.
enable	Enable the current OpenFlow instance.
flow-location	Specify the location of the flows that are used by this instance.
limit	Set the limit on resource usage by an OpenFlow instance.
listen-port	Specify the TCP port on which the OpenFlow agent of the switch waits (listens) for incoming connections from an OpenFlow controller.
max-backoff-interval	Specify the maximum interval between two consecutive attempts to connect to a controller.
member	Add member VLANs to this OpenFlow instance.
mode	Set the operation mode of the OpenFlow instance.
pipeline-model	Configure an OpenFlow instance pipeline model.
probe-interval	The probe interval is the time between two consecutive probes sent from an instance to the controller.
software-flow-table	Specify the number of software flow tables required per instance.
src-mac-grp-table	Enable the source MAC group table in the OpenFlow pipeline.

`version`	Specify the OpenFlow protocol version supported for the specific instance.

Validation rules

Validation	Error/Warning/Prompt
Destination MAC group table can be enabled on only one instance.	The destination MAC group table cannot be enabled on multiple instances.
MAC group table is supported only in standard match mode/ip-control-table mode.	The destination MAC group table is not supported in custom-pipeline mode.
In ip-control-table mode, both source MAC groups and destination MAC groups cannot be configured.	The destination MAC group table cannot be enabled when the source MAC group table is enabled in IP control pipeline mode.
When enabling the mac group table, the operational statuses of all other instances have to be down.	All the instances must be disabled before enabling the destination MAC group table.
Flow table number modification needs to be blocked when MAC group table is enabled.	Flow table number modification is not allowed when MAC group table is enabled.
MAC group feature is not available in V1 compatibility mode.	The destination MAC group table is not supported when the switch is in V1 module compatible mode.
If an instance is standard-match mode source and destination tables can be enabled. When both are enabled pipeline-model cannot be changed to ip-control.	Pipeline-model cannot be changed to ip-control if both source and destination MAC group tables are enabled.
Source and destination MAC group tables cannot be enabled when table-numbers are customized by user MAC group tables cannot be enabled.	The destination MAC group table cannot be enabled. The flow table numbers need to be reset to their default values.
When MAC group tables are configured instance pipeline-model cannot be changed to custom.	Pipeline-model cannot be changed to custom when a MAC group table is enabled.

Human readable data-path description

The OFPMP_DESC multipart response message allows an OpenFlow switch to specify a human readable text of size 255 ASCII characters.

Syntax

`openflow instance` *`inst-name`* `datapath-desc` *`datapath descrip name`*

Set a name to the data-path description field in the OFPMP_DESC message. By default, the data path description will be set to the instance name.

Example 2 Set a name to the data-path description field

```
HP-Switch(config)#  openflow instance test datapath-desc dpid1
HP-Switch(config)#  show openflow instance test

Configured OF Version        : 1.3
Negotiated OF Version        : 1.3
Instance Name                : test
Data-path Description        : dpid1
Admin. Status                : Enabled
Member List                  : VLAN 3
Pipeline Model               : Standard Match
Listen Port                  : 5555
Oper. Status                 : Up
Oper. Status Reason          : NA
Datapath ID                  : 0003a0b3ccf44fc0
Mode                         : Active
Flow Location                : Hardware and Software
No. of Hardware Flows        : 4
No. of Software Flows        : 1
Hardware Rate Limit          : 0 kbps
Software Rate Limit          : 100 pps
Conn. Interrupt Mode         : Fail-Secure
Maximum Backoff Interval     : 60 seconds
Probe Interval               : 10 seconds
Hardware Table Miss Count    : NA
No. of Software Flow Tables  : 1
Egress Only Ports            : None
Table Model                  : Policy Engine and Software

Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1                   Connected        Active            No      Equal
```

Validation table

Validation	Error/Warning/Prompt
If the number of characters in the description exceeds the limit of 255 characters.	Maximum length of the datapath description is 255 characters.

3 Group table

Groups represent sets of actions for flooding as well as more complex forwarding semantics (e.g. multipath, fast reroute, and link aggregation). As a general layer of indirection, groups also enable multiple flow entries to forward to a single identifier (e.g. IP forwarding to a common next hop). This abstraction allows common output actions across flow entries to be changed efficiently.

The group table contains group entries; each group entry contains a list of action buckets with specific semantics dependent on group type. The actions in one or more action buckets are applied to packets sent to the group. There are 4 types of groups:

1. **All**

   All the action buckets in the group should be executed when a packet hits the group table.

2. **Select**

   Execute any one action bucket in the group. The switch implementation uses round-robin to select the action bucket to be executed. Openflow specification defines a weight mechanism to do load sharing. However, this is not supported in the switch implementation. The weight MUST be given as 1. For all the other groups, weight MUST be specified as 0.

3. **Indirect**

   Execute the one defined bucket in this group. This group supports only a single bucket.

4. **Fast failover**

   Execute the first live bucket. The buckets are evaluated for liveness in the order defined by the group.

For the implementation of groups, the following is important to note:

- Group table is supported only in software. Hence, group cannot be referenced directly from a hardware flow entry.
- The number of groups per OpenFlow instance is capped to 32.
- The total number of groups in the switch is capped to 1024.
- Chaining of groups not supported. As a consequence, watch_group is also not supported while doing group additions. Watch_group MUST always be set to OFPG_ANY for all the group types.

OpenFlow groups in hardware

Group type “ALL”

Some of the OpenFlow Groups are now supported in hardware apart from the existing support in Software. The OpenFlow group type “ALL” is now supported in hardware for v2 and v3 cards.

The capabilities provided by this feature include:

- Only the type “ALL” Groups would be supported in hardware while the rest of the Groups continue to be supported in software.
- The group of type “ALL” with buckets containing output port action will be installed in hardware. If the group of type “ALL” has other actions in the buckets, then the group is installed in software.
- The ports that can be supported in OpenFlow “ALL” Group are Physical ports and LAG ports.
- The type “ALL” groups with output ports in separate buckets would be taken to hardware. If multiple output ports are given in a single bucket, the group would be put in software.

- Groups not accommodated in hardware (either because actions are not supported or because hardware resources not available) would be accommodated in software.
- Special port OFPP_FLOOD is supported in the ALL type Group in hardware.

The packet is effectively cloned for each bucket; one packet is processed for each bucket of the group.

The group bucket concept is explained below:

Bucket -1 (actions= output: a1)	Bucket-2 (actions= output: a2)	Bucket-3 (actions=output: a3)

The packets hitting the above Group action will be sent to the 3 ports (a1, a2 and a3).

4 OpenFlow per-flow rate limiting

OpenFlow supports per-flow rate-limiters for OpenFlow 1.0 as HP vendor extensions.

A rate-limiter controls the rate of packets passing through a switch. Per-flow rate-limiters associate an arbitrary number of flows with a rate-limiter. Using OpenFlow with per flow rate-limiters, any number of flows can be flexibly mapped to a rate-limiter, regardless of their source and destination ports. Rate-limiters can be used via the HP VAN SDN controller, which includes support for HP QoS extensions. Rate-limiters are addressed by a limiter_id, an arbitrary 32 bit number. Configuration of rate-limiters is done through a simple message from the controller which can add, modify or remove a rate-limiter. Flows are directed to rate-limiters through an action. Multiple flows can be associated with the same rate-limiter. Statistics can be read from the OpenFlow controller for each rate-limiter.

NOTE: Per-flow rate-limiters are used only if the hardware rate-limiter for the instance is disabled.

QoS extensions

HP QoS extension to the OpenFlow protocol provides support for rate-limiters. A rate-limiter controls the rate of packets passed through it. Per-flow rate-limiters associate an arbitrary number of flows with a rate-limiter. The HP QoS vendor extensions support per-flow rate-limiters with only drop rate flag and not the remark rate or other flags.

Create a limiter

A per-flow rate-limiter is added/created via the HP VAN SDN controller.

On receiving an OpenFlow message from the OpenFlow controller, the vendor ID is checked for a match to HP's vendor ID. If the message type received was to indicate the addition of a new rate-limiter, a new rate-limiter is created with the parameters received in the message.

Get limiter details

The details on the limiters configured can be retrieved via the HP VAN SDN controller. These details can also be checked on the switch CLI using the command `show openflow instance_name limiters`.

Support an OpenFlow with a limiter

A flow can be associated with a per-flow rate-limiter by giving the limiter ID as an OpenFlow action. For example, assume that a per-flow rate-limiter with ID 100 was created. From the HP VAN SDN controller that supports HP QoS extensions, a flow can be associated with this rate-limiter by using this limiter ID of 100 as one of the specified OpenFlow actions of that flow.

5 OpenFlow Multi-VLAN instance

Overview

OpenFlow multi-VLAN instance associates multiple VLANs to an OpenFlow instance.

The capabilities of the OpenFlow multi-VLAN instance include:

- Ability to include more than one VLAN on the switch as member VLAN for an OpenFlow instance in Virtualized mode.
- Supported on both OpenFlow 1.0 and 1.3 versions.
- For a Multi-VLAN instance, the first VLAN in the Multi-VLAN instance would be part of the DPID. Since VLANs cannot be part of multiple instances this ensures a unique DPID for each instance.
- Packet-IN for a Multi-VLAN instance would be same as aggregate mode (i.e. the Packet-IN would be sent with the VLAN tag.) If the instance is a single VLAN instance, then the behavior would be the same as the virtualized instance (i.e., the Packet-IN would be sent untagged.)
- Ability to add OpenFlow rules with wild carded VLAN in such an instance that will match traffic inbound on only those VLAN(s) which are part of the instance.
- Ability to add OpenFlow rules with a specific VLAN which is part of the VLANs in the instance.
- Supports V2 and V3 modules.

Configuration commands

Add member VLANs

Syntax

`member vlan` *`vlan-id`*

Used to add member VLANs to an instance.

Options

`no member vlan` *`vid1`* removes *`vid1`* from the multi-vlan instance. The other VLAN(s) associated with the instance would still be part of the instance. This command can take any of the following forms:

- [no]`member vlan <vid1>`
- [no]`member vlan` *`vid1, vid2, vid3`*
- [no]`member vlan` *`vid1 – vid3`*
- [no]`member vlan` *`vid1, vid3 – vid5, vid7`*

Add VLANs as members to OpenFlow instance

Syntax

[no]`openflow instance` *`INSTANCE-NAME`*`| aggregate member vlan` *`VLAN-ID-LIST`*

Add member VLANs to an OpenFlow instance. An aggregate instance is a special OpenFlow instance that includes all the VLANs on the switch except the management VLAN and controller VLAN. The `no` form deletes the instance and its configuration.

connection-interru	Set the type of behavior when the switch loses connection with the controller.
controller-id	Add controllers for an OpenFlow instance.
disable	Disable the current OpenFlow instance.
enable	Enable the current OpenFlow instance.
flow-location	Set the location of the flows used by this instance.
limit	Set limit on resource usage by an OpenFlow instance.
listen-port	Specify the TCP port on which the OpenFlow agent of the switch waits (listens) for incoming connections from an OpenFlow controller.
max-backoff-interval	Specify the maximum interval between two consecutive attempts to connect to a controller.
member	Add member VLANs to this OpenFlow instance.
mode	Set the operation mode of the OpenFlow instance.
probe-interval	The probe interval is the time between two consecutive probes sent from an instance to the controller.
software-flow-table	Specify the number of software flow tables required per instance.
version	OpenFlow protocol version supported for the specific instance.
VLAN	Add member VLANs to this OpenFlow instance.
VLAN-ID-LIST	Add member VLANs to this OpenFlow instance.

Example 3 OpenFlow instance member VLAN

```
HP-3500yl-24G(config)# openflow instance <INSTANCE-NAME> member vlan
4,45-90,120

HP-5406Rzl2(config)$ show running-config
Running configuration:
; J9850A Configuration Editor; Created on release #KB.15.17.0000x
; Ver #07:ff.f7.fc.7f.ff.3f.ef:a3
hostname "HP-5406Rzl2"
module A type j9992a
module F type j9986a
snmp-server community "public" unrestricted openflow
controller-id 1 ip 10.20.30.42 controller-interface vlan 2
  instance "t1"
    listen-port
    member vlan 3,5-7,10,20,30
    controller-id 1
    version 1.3 only
    flow-location hardware-only
    pipeline-model custom
    enable
    exit
enable
 exit

oobm
  ip address dhcp-bootp
  exit

vlan 1
  name "DEFAULT_VLAN"
  no untagged A1-A4,F23
  untagged A5-A21,F1-F22,F24
  ip address
  exit

vlan 2
  name "VLAN2"
  untagged F23
  ip address 10.20.30.40 255.255.255.0
  exit

vlan 3
  name "VLAN3"
  untagged A1-A4
  no ip address
  exit

vlan 5
  name "VLAN5"
  no ip address
  exit

vlan 6
  name "VLAN6"
  no ip address
  exit

vlan 10
  name "VLAN10"
  no ip address
  exit

vlan 30
  name "VLAN30"
  no ip address
  exit

no allow-v2-modules
HP-5406Rzl2(config)$ show openflow
OpenFlow                    : Enabled
EgressOnly Ports Mode       : Disabled

Instance Information

                  No. of     No. of      OpenFlow
Instance Name                          Oper. Status H/W Flows  S/W Flows  Version
 -------------------------------- ------------ ---------- ---------- --------
t1                                                      Up          4              0
     1.3 only
```

Validation rules

Validation rule applicable to both user mode and download mode.

Validation	Error/Warning/Prompt
Specifying a VLAN that is already a part of a different OpenFlow instance.	The VLAN specified is already a member of another OpenFlow instance, <INSTANCE-NAME>.
Specifying a VLAN that is outside the allowed VLAN range.	Invalid Input : <VLAN-ID>
Trying to delete a member which does not belong to this instance.	VLAN <VLAN-ID> is not a member of this instance
When the user tries to add the management VLAN to an OpenFlow instance.	The management VLAN cannot be a member of an OpenFlow instance
Trying to add a VLAN that is a controller interface/VLAN.	A controller interface cannot be added as a member VLAN
When a dynamic VLAN is added as a member VLAN	A dynamic VLAN cannot be added as a member VLAN.
An openFlow instance with multiple VLANs will not be supported on v1 modules and, v2 modules running in compatibility mode.	OpenFlow instances with multiple VLANs are not supported when the switch is in V1 compatible mode
User should not add member VLANs more than maximum VLANs configured on the switch.	Cannot exceed the maximum number (%s) of VLANs allowed on the switch.

Data-path description

Syntax

[no]openflow instance *instance-name* datapath-desc *string*

Specify a description for the data path.

connection-interru	Set the type of behavior when the switch loses connection with the controller.
controller-id	Add controllers for an OpenFlow instance.
disable	Disable the current OpenFlow instance.
enable	Enable the current OpenFlow instance.
flow-location	Set the location of the flows used by this instance.
limit	Set limit on resource usage by an OpenFlow instance.
listen-port	Specify TCP the port on which the OpenFlow agent of the switch waits (listens) for incoming connections from a OpenFlow controller.
max-backoff-interval	Specify the maximum interval between two consecutive attempts to connect to a controller.
member	Add members to this OpenFlow instance.
mode	Set the operation mode of the OpenFlow instance.
probe-interval	The probe interval is the time between two consecutive probes sent from an instance to the controller.
software-flow-table	Specify the number of software flow tables required per instance.

version	OpenFlow protocol version supported for the specific instance.
pipeline-model	Configure an OpenFlow instance table pipeline mode.
datapath-desc	Specify a description for the data path.

Validation rules

Validation	Error/Warning/Prompt
If the number of characters in the description exceeds the limit of 255 characters	Maximum length of the datapath description is 255 characters.

Configure table number for a flow table

This command is used to configure a table number for a flow table. If the table number is not configured, a default value is given to the table. Table number configuration is supported only on standard-match mode.

If user does not configure table number for a given table, that table will retain its default value.

If any table uses table number as 0 then we will not have the default table 0 configured in the pipeline. In standard match mode, user can configure either policy table or the first software table as table 0, when software table is configured as table 0, OpenFlow pipeline will not have HW table at all.

Standard Match Mode	
Flow Table	**Table Number**
start	0
Policy Table	100
Sw Table 1	200
Sw Table 2	201
Sw Table 3	202
Sw Table 4	203

The table numbers should be as per the following order

Standard match mode:

Pipeline start table < policy table < SW table 1 < SW table 2...

E.g.

If the policy table number is configured as 0, then there is no Pipeline start table: policy table < SW table 1 < SW table 2.

If SW table 1 is configured as table number 0, then SW table 1 < SW table 2 are present

Syntax

```
[no]openflow instance INSTANCE-NAME|aggregate table-num
HP-Switch(of-inst-t1)# table-num policy-table
```

Configure table number for flow tables.

policy-table	Specify the policy table number.
sw-table-#	Specify the software table 1 number.
<0-254>	Flow table number.

Example 4 Flow policy table

```
HP-3800-48G-PoEP-4SFPP(of-inst-t1)# table-num  policy-table
<0-254>               Flow table number.

HP-3800-48G-PoEP-4SFPP(of-inst-t1)# table-num  sw-table-1
 <0-254>               Flow table number.

HP-3800-48G-PoEP-4SFPP(of-inst-t1)# table-num  sw-table-2
<0-254>               Flow table number.

HP-3800-48G-PoEP-4SFPP(of-inst-t1)# table-num  sw-table-3
 <0-254>               Flow table number.

HP-3800-48G-PoEP-4SFPP(of-inst-t1)# table-num  sw-table-4
 <0-254>               Flow table number.
```

Validation rules

Validation	Error/Warning/Prompt
In standard match mode, default table numbers are pipeline start - 0, policy table - 100, SW table - 200. If user configures SW table number as 100, without changing policy table number, this should be blocked. To change SW table number, user should change the policy table number first and then change the SW table number.	Cannot configure the table number specified for this flow table as it is being used by %s flow table.
The table numbers should be as per the following order **Standard match mode** : Pipeline start table < policy table < SW table 1 < SW table 2... Ex. If the policy table number is configured as 0, then there is no Pipeline start table : policy table < SW table 1 < SW table 2. If SW table 1 is configured as table number 0, then SW table 1 < SW table 2 are present.	Cannot configure. Table numbers should be in increasing order.
Table number configuration is not applicable when instance is in ip-control-table or custom mode.	Cannot configure table numbers when instance is in ip-control-table/custom mode.
Software table configuration depends on maximum software-flow-table configured E.g. If maximum software-flow-table is configured as 2, then sw-table-3 and sw-table4 cannot be configured. Default value of software-flow-table is 1.	Cannot configure %s, maximum software-flow-table is %d.

Validation	Error/Warning/Prompt
If flow table numbers are non-default, instance mode cannot be changed.	Pipeline-model cannot be changed. The flow table numbers need to be reset to default values before changing the mode.
Following command need to be blocked if SW table is configured as 0. 1. openflow instance t1 flow-location hardware-only	Modifications not allowed, hardware table not present in the pipeline.

Show commands

Show OpenFlow information

You can display OpenFlow information for all instances, ports, and flows. The returned information includes the OpenFlow version supported.

Syntax

```
show openflow resources | controllers | instance
instance-name | port-statistics | flows flow-filters |
auxiliary-connections
```

Show OpenFlow information.

`resources` Shows OpenFlow resource utilization.

`controllers` Shows controllers configured for OpenFlow.

`instance-name` Instance information can be obtained for ports or flows.

`port-statistics` Shows port statistics. When a rule is executed in hardware, full statistics are no longer available for that rule. The following restrictions apply:

- byte_count is not available (software byte count only)
- Statistics are updated at a large period interval (approximately 7 seconds)
- flow_duration value is larger than the actual flow duration because of sample rate quantization

`flows` *`flow-type`*

Shows the flow table entries for a particular OpenFlow instance. The various flows displayed using *`flow-type`* are shown in “Example-Flow version 1.0” and “Example-Flow version 1.3” below.

Example-Flow version 1.0

```
(<openflow>)# show openflow instance titan flows
Flow 1 Match
  Incoming Port           : F24                  Ethernet
 Type     : IP
  Source MAC              : 000000-000000
Destination MAC  : 000000-000000
  VLAN ID                 : 0                     VLAN
Priority     : 0
  Source Protocol Address : 255.255.255.255/32
  Target Protocol Address : 128.128.128.128/32
  IP Protocol             : 0x00                  IP ToS
Bits       : 0
  Source Port              : 0
Destination Port : 0
Attributes
  Priority                : 32768                Duration
```

```
         : 10 secs
  Hard Timeout            : 0 secs               Idle
Timeout     : 60 secs
  Byte Count              : 0                    Packet
Count     : 0
  Controller ID           : 1                    Cookie
          : 0x0
  Flow Location           : Software             Hardware
 Index   : 1
  Reason Code             : 100
  Reason Description      : Rule is in hardware
Actions
  Modify Destination IP   : 183.23.45.64
  Modify Source IP        : 200.123.23.54
  Output                  : A21
```

Example-Flow version 1.3

```
(<openflow>)# show openflow instance titan flows
Flow 1
 Match
  Incoming Port           : 1/17                 Ethernet
 Type    : IP
  Source MAC              : 000000-000000
Destination MAC  : 000000-000000
  VLAN ID                 : 0                    VLAN
Priority    : 0
  Source Protocol Address : 255.255.255.255/32
  Target Protocol Address : 128.128.128.128/32
  IP Protocol             : TCP                  IP ToS
Bits      : 0
  IP ECN                  : 0                    IP DSCP
          : 18
  Source Port              : 0
Destination Port : 0
 Attributes
  Priority                : 32768                Duration
         : 10 secs
  Hard Timeout            : 0 secs               Idle
Timeout     : 0 secs
  Byte Count              : 5040                 Packet
Count     : 28
  Flow Table ID          : 3                   Controller
 ID    : 1
  Activity Count          : 0xffffffff           Cookie
          : 0x0
  Hardware Index          : 1
 Instructions
  Clear Actions
   Write Actions   Pop VLAN
         Push VLAN Decrement TTL
         Output: : 3/24, 4/5, 1/18
         Goto Table ID: 2
Flow 2
 Match
  Incoming Port           : Trk1                 Ethernet
 Type    : IPv6
  Source MAC              : 000000-000000
Destination MAC  : 000000-000000
  VLAN ID                 : 0                    VLAN
Priority    : 0
  Source Protocol Address : 255.255.255.255/32
  Target Protocol Address : 128.128.128.128/32
  IPv6 Flow Label         : 0
  IPv6 Ext. Header        : Fragment
  ND Source MAC           : 000000-000000 ND
Destination MAC  : 00000-000000
  ND Target IP            : 0:0:0:0:0:0:0:0
  IP Protocol             : 0x2C
  IP ECN                  : 0                    IP DSCP
          : 20
  Source Port              : 0
Destination Port : 0
 Attributes
  Priority                : 12345                Duration
         : 10 secs
  Hard Timeout            : 300 secs             Idle
Timeout     : 160 secs
  Byte Count              : 0                    Packet
Count     : 0
```

```
  Flow Table ID          : 6                   Controller
 ID    : 1
  Activity Count          : 0xffffffff           Cookie
          : 0x0
  Hardware Index          : 1
 Instructions
  Apply Actions
     Modify Destination IP  : 2000::5
     Modify Source IP       : 2000::6
     Modify Source MAC      : 121212-121212
     Modify Destination MAC : 131313-131313
     Modify VLAN ID         : 123
     Modify IP DSCP         : 18
     Modify IP ECN          : 1
     Decrement TTL
     Meter ID                : 112
     Group ID               : 2
  Write Actions
     Decrement TTL
     Goto Table ID          : 4
Flow 3
 Match
  Incoming Port           : 0                    Ethernet
 Type    : ARP
  Source MAC              : 000000-000000
Destination MAC  : 000000-000000
  VLAN ID                 : 0                    VLAN
Priority    : 0
  ARP Opcode              : 1
  ARP Source MAC         : 00A0C9-22B210       ARP Target
 MAC   : 000000-000000
  Source Protocol Address : 255.255.255.255/32
  Target Protocol Address : 128.128.128.128/32
 Attributes
  Priority               : 32768                Duration
         : 10 secs
  Hard Timeout            : 0 secs               Idle
Timeout     : 0  secs
  Byte Count              : 12450                Packet
Count     : 2323
  Flow Table ID          : 3                   Controller
 ID    : 3
  Activity Count          : 0xffffffff           Cookie
          : 0x0
  Hardware Index          : 1
Flow 4
 Match
  Source MAC              : 000000-000000        Ethernet
 Type    : 0x8035
  VLAN ID                 : 0
Destination MAC  : 000000-000000
  ARP Opcode              : 0                    VLAN
Priority    : 0
  ARP Source MAC          : 000000-000000
  ARP Target MAC          : 000000-000000
  Source Protocol Address : 0.0.0.0
  Target Protocol Address : 0.0.0.0
  Source IP               : 0.0.0.0
  Destination IP         : 0.0.0.0             ARP Target
 IP      : 0.0.0.0
  IPv6 Flow Label         : 0
  IPv6 Ext. Header        : None
  ND Source MAC           : 000000-000000
  ND Target IP            : 0:0:0:0:0:0:0:0      ND
Destination MAC : 000000-000000
  IP Protocol             : 0x00
  IP ECN                  : 0                    IP DSCP
            : 0
  Source Port              : 0
Destination Port   : 0
 Attributes
  Priority               : 32768                Duration
          : 15 secs
  Hard Timeout            : 0 secs               Idle
Timeout       : 50 secs
  Byte Count              : 0                    Packet
Count       : 0
  Flow Table ID          : 5                   Controller
 ID      : 5
  Activity Count          : 0xffffffff           Cookie
           : 0x0
```

```
 Hardware Index          : 1
Instructions
 Write Actions
    Output  : 2/1
    Output  : Controller
```

Where the various flows that can be shown using the *flow-type* are:

destination-ip	Show flows matching the destination IP address.
destination-mac	Show flows matching the destination MAC address.
destination-port	Show flows matching the destination port.
ethernet-type	Show flows matching the EtherType.
ip-protocol	Show flows matching the IP protocol.
ip-tos-bits	Show flows matching the IP ToS bits.
source-ip	Show flows matching the source IP address.
source-mac	Show flows matching the source MAC address.
source-port	Show flows matching the source port.
vlan-id	Show flows matching the VLAN ID.
vlan-priority	Show flows matching the VLAN priority.
destination-ipv6	Show flows matching the destination IPv6 address.
flow-table	Show flows that are hit most corresponding to the flow table number.
ingress-port	Show flows matching the ingress port.
source-ipv6	Show flows matching the source IPv6 address.

Show global OpenFlow information

Syntax

```
show openflow
```

Show OpenFlow information

Example 5 Show openflow

```
HP-Switch# show openflow

OpenFlow              : Disabled

Instance Information
                                                    No. of    No. of
  OpenFlow
Instance Name                     Oper. Status H/W Flows S/W Flows
 Version
--------------------------------- ------------ --------- ---------
 --------
titan                              Down         0         0
  1.0
marez                              Up           0         0
  1.3 only
```

Show OpenFlow instance

Syntax

```
show openflow inst inst-name
```

Show OpenFlow instance information.

Example 6 Show OpenFlow instance

```
HP-5406Rzl2(config)# show openflow instance test groups

OpenFlow Instance Groups
  Group ID                     : 2
  Group Type                   : All
   Group Location               : Hardware
  Is Hardware Counter Available : No
  Reference Count              : 1
  Packet Count                 : 0
  Byte Count                   : 0
  Duration                     : 30
  Action Buckets               : 1, 2
  Bucket 1
    Packet Count    : 0
    Byte Count      : 0
    Watch port      : Any
    Weight          : 0
    Action          : Output F22
   Bucket 2
    Packet Count    : 0
    Byte Count      : 0
    Watch port      : Any
    Weight          : 0
    Action          : Output F23

Rule pointing to above Group:
Flow 3
Match
  Incoming Port : Any                  Ethernet Type   : IP
  Source MAC    : Any                 Destination MAC : Any
  Source MAC Mask     : 000000-000000
  Destination MAC Mask     : 000000-000000
  VLAN ID       : Any                  VLAN priority   : Any
  Source IP Address        : 11.11.11.11/32
  Destination IP Address   : Any
  IP Protocol   : Any
  IP ECN        : Any                  IP DSCP         : Any
  Source Port   : Any                  Destination Port : Any

Attributes
  Priority     : 32768               Duration        : 36 seconds

  Hard Timeout : 0 seconds            Idle Timeout    : 0 seconds

  Byte Count   : NA                   Packet Count    : 0
  Flow Table ID : 100                Controller ID   : listen-port

  Cookie       : 0x0
  Hardware Index: 17

Instructions
  Apply Actions
   Group                       : 2
```

Example 7 Show OpenFlow instance

```
HP-3800-48G-4XG(of-inst-test)# sh openflow inst test

 OpenFlow Instance Flow Table Information

Configured OF Version    : 1.3
Negotiated OF Version    : 1.3
Instance Name            : test
Data-path Description   : Test network
Admin. Status            : Enabled
Member List              : VLAN 5,9,12-15
Pipeline Model           : <Standard Match | IP Control Table| Custom
Pipeline>
Listen Port              : 6633
Oper. Status             : Up
Oper. Status Reason      : NA
Datapath ID              : 0001843497ce8480
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 2
No. of Sw Flows          : 1
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : NA
No. of Sw Flow Tables    : 1
Egress Only Ports        : None
Table Model              : <None | Single Table | Policy Engine and
Software |

IP Control With Policy Engine and Software | Custom Pipeline>

Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1             Connected         Active           No     Equal
```

Show OpenFlow instance group

Syntax

`show openflow instance` *`inst-name`* `groups`

Example 8 Show openflow instance group

```
HP-Switch(of-inst-test)# show openflow instance test groups

 OpenFlow Instance Groups

   Group ID                      : 1
   Group Type                    : All
   Group Location                : Hardware
   Is Hardware Counter Available: Yes
   Reference Count               : 0
   Packet Count                  : 0
   Byte Count                    : 0
   Duration                      : 22
   Action Buckets                : 1, 2
      Bucket 1
         Packet Count     : 0
         Byte Count       : 0
         Watch port       : Any
         Weight           : 0
         Action           : Set Field Ethernet Source 2:2:2:2:3:3

                            Output 1
      Bucket 2
         Packet Count     : 0
         Byte Count       : 0
         Watch port       : Any
         Weight           : 0
         Action           : Output 3
```

Show group information for a specific instance

Syntax

`show openflow instance` *`instance-name`* `|` `aggregate groups` *`group-ID`*

Displays group information for a specific instance.

Show OpenFlow resources

Syntax

`show openflow resources`

Show OpenFlow resource usage in Policy Enforcement Engine.

Example 9 Show openflow resources

```
HP-Switch(config)# show openflow resources

Resource usage in Policy Enforcement Engine

               |   Rules    |  Rules Used
         Ports | Available | ACL | QoS | IDM |  VT | Mirr | PBR |  OF  |
 Other |

--------------+-----------+-----+-----+-----+-----+------+-----+------+-------|

 1-24          |      3052 |   0 |   0 |   0 |   0 |    0 |   0 |    3 |
     0 |

               |   Meters   |  Meters Used
         Ports | Available | ACL | QoS | IDM |  VT | Mirr | PBR |  OF  |
 Other |

--------------+-----------+-----+-----+-----+-----+------+-----+------+-------|

 1-24          |       254 |     |   0 |   0 |     |      |     |    1 |
     0 |

               |Application|
               |Port Ranges|  Application Port Ranges Used
         Ports | Available | ACL | QoS | IDM |  VT | Mirr | PBR |  OF  |
 Other |

--------------+-----------+-----+-----+-----+-----+------+-----+------+-------|

 1-24          |        14 |   0 |   0 |   0 |     |    0 |   0 |      |
     0 |

 2 of 8 Policy Engine management resources used.

Resource usage in Custom Pipeline Engine:

               |   Tables      | Tables
         Slot  |   Available   | Used
 --------------+---------------+---------+
           A   |      32       |   0     |

               |   Action-Set  | Action-Set
         Slot  |   Available   | Used
 --------------+---------------+---------+
           A   |      8176     |   0     |

               |   Meters      | Meters
         Slot  |   Available   |  Used
 --------------+---------------+---------+
           A   |      2000     |   0     |

               |   Counters    | Counters
         Slot  |   Available   |  Used
 --------------+---------------+---------+
           A   |      32000    |   0     |

 Key:
 ACL = Access Control Lists
 QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits

 IDM = Identity Driven Management
 VT  = Virus Throttling blocks
 Mirr = Mirror Policies, Remote Intelligent Mirror endpoints
 PBR = Policy Based Routing Policies
 OF = OpenFlow
 Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU,
         Transparent Mode, RA Guard.
```

NOTE: Resource usage includes resources actually in use, or reserved for future use by the listed feature. Internal dedicated-purpose resources, such as port bandwidth limits or VLAN QoS priority, are not included.

Show OpenFlow controllers

Displays OpenFlow controllers configured for use by OpenFlow.

Syntax

```
show openflow controllers
```

Example-show openFlow controllers

```
HP Switch(config)# show openflow controllers

Controller Information

Controller Id IP Address        Port   Interface
----------------------------- ------ ---------
1             20.0.0.2           6633   VLAN 6
```

Show flow table information

These commands display per instance flow table information, including both hardware and software flow tables.

NOTE: This option is available only for instances running OpenFlow version 1.3.

Viewing OpenFlow instance flow-table

Syntax

```
show openflow instance inst-name flow-table
```

Example 10 Show flow table

```
HP-Switch(of-inst-test)# show openflow instance test flow-table

 OpenFlow Instance Flow Table Information

Table                          Flow       Available Free  Miss
ID     Table Name              Count      Flow Count      Count
Goto Table
------ ---------------------- ---------- -----------    -----------
------------
 0      Start                   1          0              0            *
 100    Policy Table            1          8000           34           200

 200    SW Table 1              1                         10           *

 * Denotes that the pipeline could end here.
```

Viewing global flow table information

Syntax

```
show openflow flow-table
```

Displays global flow table information.

Example 11 Display OpenFlow flow tables

```
HP-5406zl(of-inst-t1)# show openflow flow-table

Flow Table Information

                                                  Max.      Refresh
     Flow
Table Name               Usage     Rate (seconds)   Count
------------------------ --------- --------------  ------
IP Control Table         50%   12              0
Policy Engine Table      50%   20              0

             IP Control Table    Policy Engine Table
Slot ID   Current Usage (%)   Current Usage (%)
-------- -----------------   -------------------
1           0.000000              0.07
6           0.000000              0.07
```

Note: Current usage is percentage of OpenFlow maximum usage

Viewing specific table capability

Syntax

`show openflow instance` *`instance-name`* `|aggregate flow-table` *`table-id`* `table-capability`

Shows OpenFlow table capability information for a specific flow table ID.

Example 12 Display OpenFlow flowtable capability

```
show openflow instance test flow-table 50 table-capability

OpenFlow IP Control Table

Table Match Capabilities:
   VLAN ID
   Source IPv4, IPv6
   Destination IPv4, IPv6
Table Instructions:
   Goto Table 101
Table-Miss Instructions:
   *Goto Table 102

*Currently configured action for table-miss flow.

show openflow instance test flow-table 101 table-capability

OpenFlow Accelerated Table

Table Match Capabilities:
   Incoming Port                  Ethernet Type: IPv4, IPv6
   VLAN ID                        VLAN Priority
   Source IPv4, IPv6              Destination IPv4, IPv6
   IPv6 Flow Label
   IP Protocol                    IP DSCP
   Source Port                    Destination Port
   ICMPv4 Type                    ICMPv4 Code
Table Instructions:
   Metering
      Band Type
         Drop
         Remark DSCP
   Apply-Actions
      Set-Field
         VLAN ID
         VLAN Priority
         Strip VLAN ID
         Source MAC
         Destination MAC
         IP DSCP
      Output
        Switch Port, Drop, Normal
Table-Miss Instructions:
   Apply-Actions
      Output
        Drop, Normal
   *Goto Table 200

*Currently configured action for table-miss flow.


show openflow instance test flow-table 200 table-capability

OpenFlow Software Table 1

Table Match Capabilities:
   Incoming Logical Port              Incoming Physical Port
   Metadata                           Destination MAC
   Ethernet Type                      Source MAC
   VLAN ID                            VLAN Priority
   IP DSCP                            IP ECN
```

```
   IP Proto
   Source IPv4, IPv6                    Destination IPv4, IPv6

   Source Port                          Destination Port
   IPV6 Flow Label
   Source SCTP Port                     Destination SCTP Port
   ICMPv4 Type                          ICMPv4 Code
   ARP Opcode
   ARP Source IPv4                      ARP Destination IPv4
   ARP Source MAC                       ARP Destination MAC
   ICMPv6 Type                          ICMPv6 Code
   IPv6 ND SLL                          IPv6 ND TLL
   ND IPv6 Target
Table Instructions:
   Apply-Actions
      Set-Field
         VLAN ID                        VLAN Priority
         Strip VLAN
         Source MAC                     Destination MAC
         Set TTL                        Decrement TTL
         IP ECN                         IP DSCP
      Output
         Drop, Normal
   Clear-Actions
   Write-Actions
   Write-Metadata
Table-Miss Instructions:
   Apply-Actions
      Output
         Drop, Normal
   Goto Table-201, *202, 203, 204

*Currently configured action for table-miss flow.
```

Viewing group table information

Syntax

`show openflow instance` *`instance-name`* `| aggregate groups` *`group-id`*

Displays OpenFlow group table information. Groups are supported in software tables only. Up to 4 types of groups are supported with 32 groups supported per instance and 1024 groups across all instances. A select group uses the round-robin method for every packet and the number of action buckets are capped to 8 per group.

Example 13 Display OpenFlow groups

```
show openflow instance instance-name |aggregate groups
Group ID         : 1
Group Type       : ALL
Reference Count  : 32767
Packet Count     : 0
Byte Count       : 0
Duration         : 10 seconds
Action Buckets   : 1, 2
 Bucket 1
  Packet Count     : 0
  Byte Count       : 0
  Watch port       : Any
  Weight           : 0
  Actions          : output A1
 Bucket 2
   Actions    :output F2
  Packet Count     : 0
  Byte Count       : 0
  Watch port       : Any
  Weight           : 0
  Action           : Output F23

Group ID : 1
Group Type : SELECT
Reference Count: 0Packet Count: 0
Byte Count: 0
Duration: 10
Action Buckets: 1
 Bucket 1:
  Packet Count: 0
  Byte Count: 0
  Watch Port: Any
  Weight: 1
  Actions: output A

Group ID: 7
Group Type: INDIRECT
Reference Count: 0
Packet Count: 0
Byte Count: 0
Duration: 10
Action Buckets: 1
 Bucket 1
  Packet Count: 0
  Byte Count: 0
  Watch Port: Any
  Weight: 0
  Actions: output A1
Group ID: 32
 Group Type: FAST
  FAIL OVER
Reference Count: 0
Packet Count: 0
Byte Count: 0
Duration: 10
Action Buckets: 1
 Bucket 1
  Packet Count: 0
  Byte Count: 0
  Watch port: A1
  Weight: 0
  Actions: output A1
```

Show meter information for a specific instance

Displays meter information. Meters are instance-specific. Meters are only supported in hardware tables and the maximum number of meters differs between platforms. DSCP remark meter is supported only in standard match mode. Further, DSCP remark type band meter cannot be attached to flows with a non-IP match.

NOTE: When a same OpenFlow meter is used two or more times in an OpenFlow pipeline, it will result in the meter rates to be skewed leading to unpredictable behavior in how the packets are metered. HP recommends not using a meter more than once in a packet pipeline to avoid undesired behaviors.

Syntax

```
show openflow instance instance-name | aggregate meters
```

Example-Display meters for an OpenFlow instance

```
HP-3800-24SFP-2SFPP# show open instance t3 meters

OpenFlow Instance Meters
Meter ID : 1
Flow Count : 1
Input Packet Count : 0
Duration : 0

          Packet
Band Type Rate         Count
--------- ------------ --------
Drop      150 kbps      0
```

v3 Push/Pop VLAN

HP switches running OpenFlow do not support Push and Pop VLANs. However, additional or modified tags are supported for single-tagged packets.

Supported	Not Supported
On all OpenFlow instance pipelines.	On v1 mode of operation.
On v2 and v3 modes of operation.	Push VLAN action does not support double tagging.
Push VLANs supported only with ether-type of 0x8100 (802.1q).	Push VLAN, Set Field and VLAN VID are not supported in the same flow.
Push VLAN action modifies and existing 802.1q tag in the packet.	N/A
Pop VLAN action strips the 802.1q tag from the packet.	N/A

Show auxiliary connection information

Only one auxiliary connection is supported per main controller connection.

Syntax

```
show openflow auxiliary-connections
```

Displays auxiliary connection information.

Example-Display OpenFlow auxiliary connections

```
show openflow auxiliary-connections

Auxiliary
Conn. Index Type Port
----------- ---- ----
1           TCP  7777
2           UDP  8888
```

Show per flow rate limiter information

Syntax

`show openflow instance instance-name | aggregate limiters`

Displays per-flow rate limiters information.

Example-Display per-flow rate-limiters for an OpenFlow instance

```
HP-3500yl-24G-PoEP# show openflow instance test limiters

OpenFlow Instance Per Flow Rate Limiters
Maximum Limiters  :  256

                                    Rate
Limiter ID   Action    (kbps)          Flow Count
----------   ------    ----------   ----------
112              Drop       128             2
```

Show group table information

Viewing multiport-filter-limit

Syntax

`show openflow multiport-filter-limit`

Displays multiport filter information. (Only in OpenFlow version 1.3.)

Example-Viewing multiport filter information

```
HP-Switch# show openflow multiport-filter-limit

Total Multiport Filters: 4096

             Filters     Filters     Filters
Features     Allocated   Used        Free
------------ ----------- ----------- -----------
OpenFlow     2048        1500        500
```

Show statistics

Viewing port statistics per instance

Syntax

`show openflow instance instance-name | aggregate port statistics`

Displays port statistics information per instance.

Example-Display port statistics for version 1.3

```
HP-Switch# show openflow instance test port-statistics
Number of Ports: 2
```

```
Port 47: Up
 Status
  Admin. Status   : Enabled             Flood       : Enabled
  Receive         : Enabled             Forward     : Enabled
  Packet_in       : Enabled
 Statistics
  Collisions      : 0
  Rx Packets      : 0                   Tx Packets  : 68
  Rx Bytes        : 0                   Tx Bytes    : 8066
  Rx Dropped      : 0                   Tx Dropped  : 0
  Rx Errors       : 0                   Tx Errors   : 0
  Frame Errors    : 0
  CRC Errors      : 0
  Overrun Errors  : 0
  Port 48: Down
 Status
  Admin. Status   :                      Flood       :
  Receive         :                      Forward     :
  Packet_in       :
 Statistics
  Collisions      :
   Rx Packets      : 0                  Tx Packets  : 0
     Rx Bytes        : 0                  Tx Bytes    : 0
   Rx Dropped      : 0                  Tx Dropped  : 0
   Rx Errors       : 0                  Tx Errors   : 0
   Frame Errors    : 0
     CRC Errors      : 0
   Overrun Errors  : 0
```

Viewing message statistics for an instance

This command displays statistics for flow, port, group and meter modification message from the controller, the number of modification messages received from the controller and the number of messages rejected.

Syntax

`show openflow instance` *`instance-name`* `| aggregate message-statistics`

Show message statistics information for an instance. This displays the number of OpenFlow modification messages received from the controller and the number of messages rejected by the switch.

Example-Display message-statistics for an OpenFlow instance

```
OpenFlow #: show openflow instance instance-name message statistics
OpenFlow
Message Type    Received Rejected
--------------- -------- --------
OFPT_FLOW_MOD   100      12
OFPT_PORT_MOD   120      22
OFPT_GROUP_MOD  22       2
OFPT_METER_MOD  12       0
```

Show OpenFlow instance capabilities information

Syntax

`show openflow instance` *`instance-name`* `| aggregate capabilities`

Displays OpenFlow instance capabilities.

Example-Display OpenFlow instance capabilities information

```
HP-3500yl-24G-PoEP# show openflow instance test capabilities

Policy Engine Match Capability : Extended Match

Switch Capabilities
--------------------
Flow Statistics
Table Statistics
Port Statistics
Group Statistics
Blank Ports
```

6 OpenFlow custom pipeline

Custom pipeline mode

The OpenFlow controller can carve out flow tables dynamically by enabling the switch to accept requests from the controller.

The controller uses the `OFPMP_TABLE_FEATURES` request message to configure the tables in the OpenFlow switch. The custom pipeline is created in hardware via the command “pipeline-model custom” only if the version of the instance is 1.3. This feature is supported on v3 modules only and when the switch is running in v3-only mode.

The capabilities provided by this feature include:

- Controllers can carve out tables with specific match & action parameters in the custom mode.
- All the tables for this mode are created in the hardware.
- Supports rules with various instructions APPLY, WRITE, CLEAR, METER and GOTO
- Supports more packet modifications.
- Supports two types of tables i.e. HASH and TCAM.
- If the size of the tables requested by controller cannot be accommodated in hardware, the request would be rejected.
- The Legacy Policy, IP-control tables and the Software tables are not part of this pipeline.
- Maximum of 8 tables can be configured per instance by the controller.
- The following fields are matched in the Custom Pipeline Instance:
    - OFPXMT_OFB_IN_PORT
    - OFPXMT_OFB_ETH_DST
    - OFPXMT_OFB_ETH_SRC
    - OFPXMT_OFB_ETH_TYPE
    - OFPXMT_OFB_VLAN_VID
    - OFPXMT_OFB_VLAN_PCP
    - OFPXMT_OFB_IP_DSCP
    - OFPXMT_OFB_IP_PROTO
    - OFPXMT_OFB_IPV4_SRC
    - OFPXMT_OFB_IPV4_DST
    - OFPXMT_OFB_TCP_SRC
    - OFPXMT_OFB_TCP_DST
    - OFPXMT_OFB_UDP_SRC
    - OFPXMT_OFB_UDP_DST

    - OFPXMT_OFB_IPV6_SRC
    - OFPXMT_OFB_IPV6_DST
- The following packet modifications are supported in the Custom Pipeline Instance:
- OFPXMT_OFB_ETH_SRC
- OFPXMT_OFB_ETH_DST
- OFPXMT_OFB_VLAN_VID
- OFPXMT_OFB_VLAN_PCP
- OFPXMT_OFB_IPV4_SRC
- OFPXMT_OFB_IPV4_DST
- OFPXMT_OFB_IP_DSCP
- OFPXMT_OFB_TCP_SRC
- OFPXMT_OFB_TCP_DST
- OFPXMT_OFB_UDP_SRC
- OFPXMT_OFB_UDP_DST
- The following output port actions are supported in Custom Pipeline Instance:
- PHYSICAL and TRUNK PORTs
- GRE TUNNEL
- MIRROR
- OFPP_CONTROLLER
- OFPP_FLOOD
- GROUP
- MULTIPORT (Output to multiple physical ports)
- OFPP_NORMAL

Default Pipeline in custom mode

The table pipeline is created in the hardware in the CLI by using the command `pipeline-model custom`.

Figure 13 Table pipeline



Only one instance can be enabled in the custom mode by default. OpenFlow hardware resources are allocated to the first OpenFlow instance enabled. If the controller reduces the table size for an instance then other instances can be enabled using the customer mode. The default pipeline, in custom mode, is advertised by the switch consisting of 3 Hash tables and 1 TCAM table as shown in Figure 5 above. Hash tables 0, 1, 2 and TCAM table 3 are represented below.

Table 5 Hash tables 0 & 1

Table-Number/ Property	Table-0 (Hash)	Table-1 (Hash)
Match Key	OFPXMT_OFB_VLAN_VID & OFPXMT_OFB_ETH_SRC	OFPXMT_OFB_VLAN_VID & OFPXMT_OFB_ETH_DST
Instructions	Apply-actions, Clear-actions, Write-actions, Meter & Goto-Table	Apply-actions, Clear-actions, Write-actions, Meter & Goto-Table
Scale	8k	8k

Table 6 Hash table 2 & TCAM table 3

Table-Number/ Property	Table 2 (Hash)	Table 3 (TCAM)
Match Key	OFPXMT_OFB_ETH_TYPE,	OFPXMT_OFB_ETH_TYPE,
	OFAL_XMT_OFB_VLAN_VID,	OFPXMT_OFB_VLAN_VID,
	OFPXMT_OFB_IPV4_SRC,	OFPXMT_OFB_VLAN_PCP,
	OFPXMT_OFB_IPV4_DST,	OFPXMT_OFB_ETH_SRC,
	OFAL_XMT_OFB_IPV6_SRC,	OFPXMT_OFB_ETH_DST,
	OFAL_XMT_OFB_IPV6_DST,	OFPXMT_OFB_IPV4_SRC,
	OFPXMT_OFB_IP_PROTO,	OFPXMT_OFB_IPV4_DST,
	OFPXMT_OFB_TCP_SRC,	OFAL_XMT_OFB_IPV6_SRC,
	OFPXMT_OFB_TCP_DST,	OFAL_XMT_OFB_IPV6_DST,
	OFPXMT_OFB_UDP_SRC,	OFPXMT_OFB_IP_DSCP
	OFPXMT_OFB_UDP_DST	OFPXMT_OFB_IP_PROTO,
		OFPXMT_OFB_TCP_SRC,
		OFPXMT_OFB_TCP_DST,
		OFPXMT_OFB_UDP_SRC,
		OFPXMT_OFB_UDP_DST
	Apply-actions, Clear-actions, Write-actions, Meter & Goto-Table	Apply-actions, Clear-actions, Meter & Write-actions
	8k	2k

Pipeline modification process

Pipeline modification follows this basic process:

1. An instance must be configured in the custom mode so that the controller can use the table modifications feature.
2. A table modification request is triggered by the controller using the “Table Features” request message.
3. The first “OFPMP_TABLE_FEATURES” is sent with an empty body and the switch replies with the default table pipeline.
4. The controller understands the current pipeline.

   If the controller wants to modify the default table pipeline, it again sends “OFPMP_TABLE_FEATURES” with the required table pipeline configuration.

5. The table pipeline would have details of the table numbers, size of each table, instructions/match/action capabilities of each table.
6. If the table pipeline with all its properties and scale can be achieved in the hardware, the table modification request is accepted.
7. The table modification can happen dynamically on custom pipeline instances (i.e. instance need not have to be disabled to do the table modification.)

Figure 14 Openflow pipeline

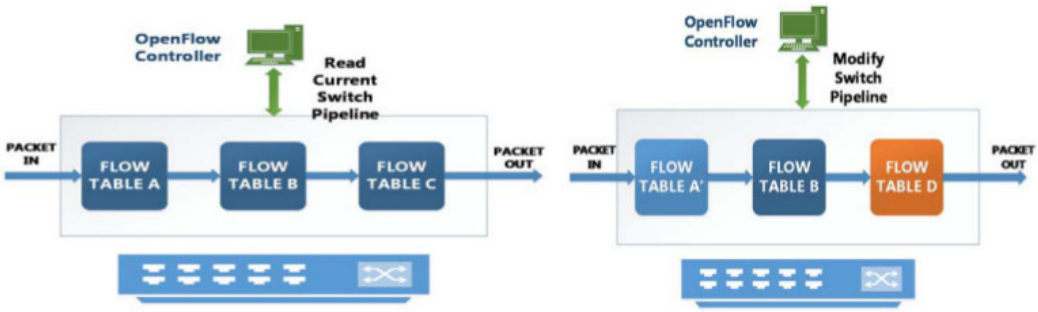
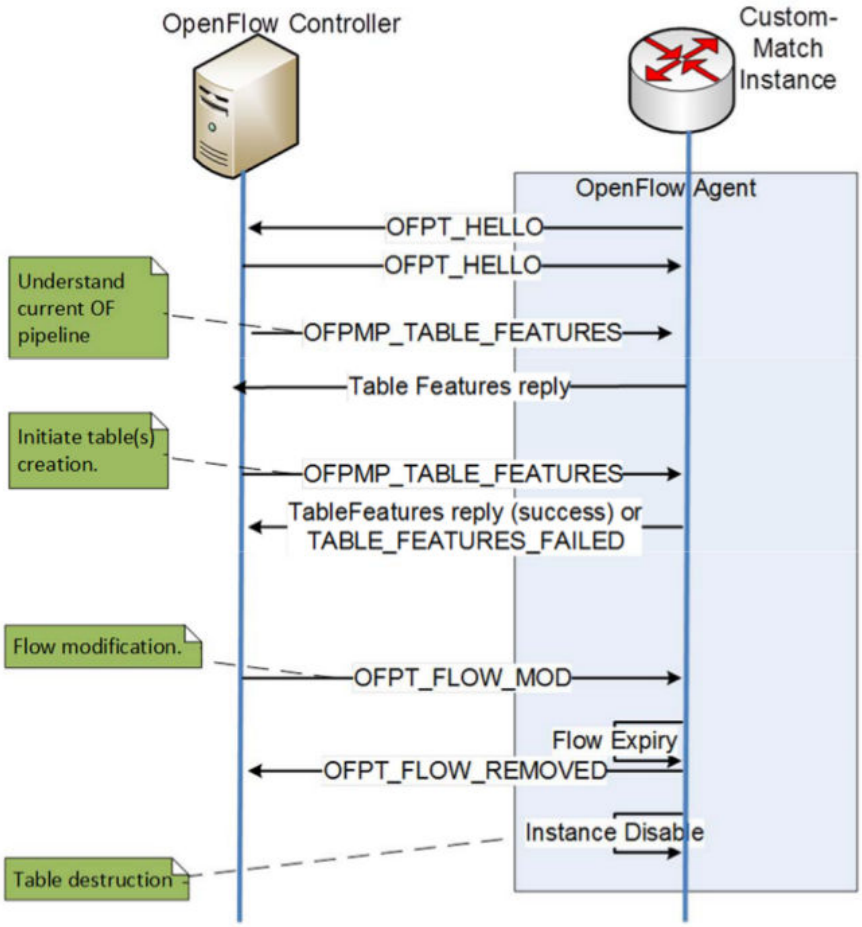


Figure 15 OpenFlow custom match instance



Example 14 Custom Pipeline Instance

```
HP-5406Rzl2(openflow)$ show running-config

Running configuration:
; J9850A Configuration Editor; Created on release #KB.15.17.0000x
; Ver #07:ff.f7.fc.7f.ff.3f.ef:a3
hostname "HP-5406Rzl2"
module A type j9992a
module F type j9986a
snmp-server community "public" unrestricted

openflow
  controller-id 1 ip 10.20.30.42 controller-interface vlan 2
  instance aggregate
    listen-port
    controller-id 1
    version 1.3 only
    pipeline-model custom
    enable
    exit
    enable

oobm
  ip address dhcp-bootp
  exit

vlan 1
  name "DEFAULT_VLAN"
  no untagged F23
  untagged A1-A21,F1-F22,F24
  ip address dhcp-bootp
  exit

vlan 2
  name "VLAN2"
  untagged F23
  ip address 10.20.30.40 255.255.255.0
  exit

no allow-v2-modules
HP-5406Rzl2(openflow)$ show openflow instance aggregate
Configured OF Version   : 1.3 only
Negotiated OF Version   : 1.3
Instance Name           : aggregate
Data-path Description   : aggregate
Admin. Status           : Enabled
Member List             : VLAN 1
Pipeline Model          : Custom Pipeline
Listen Port             : 6633
Oper. Status            : Up
Oper. Status Reason     : NA
Datapath ID             : 0001a01d488f2700
Mode                    : Active
Flow Location           : Hardware Only
No. of Hw Flows         : 4
No. of Sw Flows         : 0
Hw. Rate Limit          : 0 kbps
Sw. Rate Limit          : 100 pps
Conn. Interrupt Mode    : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval          : 10 seconds
Hw. Table Miss Count    : NA
No. of Sw Flow Tables   : NA
Egress Only Ports       : None
Table Model             : Custom Pipeline


Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1               Connected           Active             No     Equal
```

```
HP-5406Rzl2(openflow)$ show openflow instance aggregate flow-table
OpenFlow Instance Flow Table Information

Table                              Flow     Available   Free  Miss
ID     Table Name                 Count    Flow Count      Count            Goto Table
------ ---------------------- -------- -------------- ------------ -------------
0      Custom L2 Src             1          9829            0               1, 2, 3
1       Custom L2 Dst             1          9829             0                2, 3
2       Custom L3 Table          1          9829            0                3
3       Custom TCAM Table        1          2015             0                *
```

* Denotes that the pipeline could end here

```
HP-5406Rzl2(openflow)$ show openflow instance aggregate flow-table

OpenFlow Instance Flow Table Information
Table                              Flow     Available    Free Miss
ID     Table Name                 Count    Flow Count      Count          Goto Table
------ ---------------------- -------- -------------- ------------ -------------
0      Custom L2 Src             1          9829             0              1, 2, 3
1       Custom L2 Dst            1         9829            0              2, 3
2       Custom L3 Table          1          9829             0              3
3       Custom TCAM Table        1         2015            0               *
```

* Denotes that the pipeline could end here.

Scale on custom pipeline Instance

- The hardware can match 4 different Groups of match in the custom-pipeline mode.
- The number of groups depend on the on the match fields in the HASH or TCAM table.

Group 1	IN PORT	MAC SA	MAC DA	ETHER TYPE		
Group 2	IP SA (IPv4 & IPv6)					
Group 3	VLAN ID	VLAN PCP	IP DSCP	IP PROTO	TCP/UDP SRC PORT	TCP/UDP DST PORT
Group 4	IP DA (IPv4 & IPv6)					

HASH table

- A single hash table can have match fields from any of the above 3 groups only.
- Based on the number of groups matched, the scale will vary
    - If the hash table is created with match fields from one group, then it can hold up to 64k entries
    - If the hash table is created with match fields from two or three groups, then it can hold up to 32k entries.

TCAM table

- A single tcam table can have match fields from all the 4 groups.
- The number of groups would depend on the on the match fields in the tcam table.
- Hence the scale would vary depending on the number of groups
    - If the tcam table is created with match fields from one group, then it can hold up to 8k entries.
    - If the tcam table is created with match fields from two groups, then it can hold up to 4k entries
    - If the tcam table is created with match fields from three or four groups, then it can hold up to 2k entries

---

NOTE: An instance without “pipeline-model” configured defaults to standard-match but will change to ip-control mode when ip-control-mode globally enabled.

An instance with “pipeline-model” configured as standard-match will not change to ip-control mode when ip-control-mode is globally enabled.

---

7 Administering OpenFlow

Setting OpenFlow statistics refresh interval

Choose the maximum time interval before hardware statistics are refreshed.

Syntax

`openflow hardware-statistics refresh-interval`*`secs`*

`secs` The hardware statistics refresh-interval for OpenFlow.

Default: 20 seconds

Range: 0— 3600 seconds

NOTE: With value of 0, the hardware is no longer polled to update the statistics. Refresh-rate used in the command has been depreciated.

Refresh interval policy-engine table

Syntax

`hardware-statistics refresh-interval policy-engine-table`

Set the hardware statistics refresh interval for OpenFlow. Specify the policy engine table refresh interval. A value of 0 means that the hardware is no longer being polled to update the statistics.

policy-engine-table	Specify the policy engine table refresh interval.
<0-3600>	The refresh interval.

Custom table numbering

Enables a user to configure custom table numbers for tables in an OpenFlow pipeline. If the table number is not configured, a default value is given to the table.

Syntax

[no]`openflow instance` *`inst-name`*`|aggregate` *`table-num`*

Configure custom table-number.

policy-table	Specify the policy table number.
table-num	Specify the software table 1 number.
<0-251>	Flow table number.

Example 15 Configure table number for flow tables.

```
HP-Switch(of-inst-t1)# table-num policy-table
```

Example 16 Changing the table-number for a policy-table

```
HP-5406zl(of-inst-t1)# table-num policy-table 1
HP-5406zl(of-inst-t1)# enable
HP-5406zl(of-inst-t1)# show openflow instance t1 flow-table

OpenFlow Instance Flow Table Information
Table                            Flow     Available Free  Miss
ID     Table Name              Count    Flow Count       Count
 Goto Table
----- ---------------------- -------- ---------------- -------------
----------------
0      Start                     1         NA               0
     1
1     Policy Table             1         NA               0
   200
200   SW Table        1             1               0                *
* Denotes that the pipeline could end here.
```

Example 17 Policy table as the first table in the instance.

```
HP-5406zl(of-inst-t1)# table-num policy-table 0
HP-5406zl(of-inst-t1)# enable
HP-5406zl(of-inst-t1)# show openflow instance t1 flow-table

OpenFlow Instance Flow Table Information
Table                            Flow     Available Free  Miss
ID     Table Name              Count    Flow Count       Count
 Goto Table
----- ---------------------- -------- ---------------- -------------
----------------
0      Policy Table             1        NA               0
    200
200    SW Table 1               1         NA               0
    *
* Denotes that the pipeline could end here.
```

Example 18 Software table as the first table in the instance.

```
HP-5406zl(of-inst-t1)# disable
HP-5406zl(of-inst-t1)# no table-num policy-table
HP-5406zl(of-inst-t1)# table-num sw-table-1 0
HP-5406zl(of-inst-t1)# enable
HP-5406zl(of-inst-t1)# show openflow instance t1 flow-table

OpenFlow Instance Flow Table Information
Table                            Flow     Available Free  Miss
ID     Table Name              Count    Flow Count       Count
 Goto Table
----- ---------------------- -------- ---------------- -------------
----------------
0      SW Table 1              1           NA               2
    *
* Denotes that the pipeline could end here.
```

Implementation notes

- Custom table numbering command is supported only on Standard match mode instances.
- This feature is not supported on OpenFlow v1.0 instances.

- Different OpenFlow instances can have different table numbers for a given table.
- A ‘no’ version of the command will restore the table number to its default value.
- Only policy-table and SW-table-1 can configured as the first table in standard match mode pipeline.
- The default table numbers in a standard match mode instance are

Standard Match Mode	
Flow Table	**Table Number**
Start	0
Policy Table	100
Sw Table 1	200
Sw Table 2	201
Sw Table 3	202
Sw Table 4	203

Validation rules

Validation	**Error/Warning/Prompt**
In standard match mode, default table numbers are pipeline start - 0, policy table - 100, SW table - 200. If user configures SW table number as 100, without changing policy table number, this should be blocked. To change SW table number, user should change the policy table number first and then change the SW table number.	Cannot configure the table number specified for this flow table as it is being used by %s flow table.
The table numbers should be as per the following order **Standard match mode** : Pipeline start table < policy table < SW table 1 < SW table 2... Ex. If the policy table number is configured as 0, then there is no Pipeline start table : policy table < SW table 1 < SW table 2. If SW table 1 is configured as table number 0, then SW table 1 < SW table 2 are present.	Cannot configure. Table numbers should be in increasing order.
Table number configuration is not applicable when instance is in ip-control-table or custom mode.	Cannot configure table numbers when instance is in ip-control-table/custom mode.
Software table configuration depends on maximum software-flow-table configured E.g. If maximum software-flow-table is configured as 2, then sw-table-3 and sw-table4 cannot be configured.	Cannot configure %s, maximum software-flow-table is %d.

Validation	Error/Warning/Prompt
Default value of software-flow-table is 1.	
If flow table numbers are non-default, instance mode cannot be changed.	Pipeline-model cannot be changed. The flow table numbers need to be reset to default values before changing the mode.
Following command need to be blocked if SW table is configured as 0. 1. openflow instance t1 flow-location hardware-only	Modifications not allowed, hardware table not present in the pipeline.

8 Troubleshooting OpenFlow

Diagnostic Tools Overview and Usage

Debug OpenFlow

You can display OpenFlow protocol packets or event description.

NOTE: The `debug openflow packets` option only displays OpenFlow protocol packets exchanged between the switch and the controller.

Syntax

```
HP Switch# debug openflow <errors|events|instance|packets>
```

errors	Display OpenFlow error messages.
events	Enable debug messages for all OpenFlow events like addition/deletion/modification, enable/disable etc.
instance	Specify an OpenFlow instance for instance-specific debug messages.
packets	Enable debug messages for all OpenFlow packets.

Example-Debug logs

Flow deletion

```
mOFCtrlTask: 00020| DBG|Flow deletion:
idle_timeout=60,dl_type=0x0800,in_port=27,dl_vlan=65535,
dl_vlan_pcp=0,dl_src=00:50:56:9f:5f:0a,dl_dst=00:50:56:9f:19:92,
nw_src=1.2.3.6,nw_dst=1.2.3.4,icmp_type=0,icmp_code=0,
actions=output:26
```

Flow addition

```
mOFCtrlTask: 00019| DBG|Flow addition:
idle_timeout=60,dl_type=0x0800,in_port=27,
dl_vlan=65535,dl_vlan_pcp=0,dl_src=00:50:56:9f:5f:0a,
dl_dst=00:50:56:9f:19:92,nw_src=1.2.3.6,nw_dst=1.2.3.4,
icmp_type=0,icmp_code=0,actions=output:26
```

Flow expiry

```
mOFCtrlTask: 00018| DBG|Flow expiry:
idle_timeout=1200,dl_type=0x0800,nw_src=1.2.3.7,
nw_dst=1.2.3.8,actions=mod_nw_src:9.8.7.6
```

Error messages

Interoperability error messages

Enabling OpenFlow

Enabling OpenFlow when Meshing is enabled will result in an error message similar to the following.

```
OpenFlow cannot be enabled when Meshing is configured.
```

Enabling meshing

Enabling meshing when OpenFlow is enabled will result in an error message similar to the following.

```
Meshing cannot be configured when OpenFlow is enabled.
```

Enable OpenFlow with QinQ

Enabling OpenFlow when Q-in-Q is enabled will result in an error message similar to the following.

```
OpenFlow cannot be enabled when Q-in-Q is configured.
```

Enabling QinQ with OpenFlow

Enabling Q-in-Q when OpenFlow is enabled will result in an error message similar to the following.

```
Q-in-Q cannot be configured when OpenFlow is enabled.
```

Enabling transparent mode

Enabling Transparent Mode (TRmode) when OpenFlow is enabled will result in an error message similar to the following.

```
Transparent Mode cannot be enabled when OpenFlow is enabled.
```

Enabling OpenFlow with transparent mode

Enabling OpenFlow when Transparent Mode is enabled will result in an error message similar to the following.

```
OpenFlow cannot be enabled when Transparent Mode is enabled.
```

Enabling remote mirror endpoint

Enabling Remote Mirror Endpoint when OpenFlow is enabled generates an error message similar to the following.

```
Remote Mirror Endpoint cannot be configured when OpenFlow
is enabled.
```

Enabling OpenFlow with remote mirror endpoint

Enabling OpenFlow when Remote Mirror Endpoint is enabled generates an error message similar to the following.

```
OpenFlow cannot be enabled when Remote Mirror Endpoint is
configured.
```

Adding a port

Adding a port to a trunk that is part of an OpenFlow member VLAN generates an error message similar to the following.

```
Trunk in use by an OpenFlow instance may not be modified.
```

Deleting a port

Deleting a port from a trunk that is part of an OpenFlow member VLAN generates an error message similar to the following.

```
Trunk in use by an OpenFlow instance may not be modified.
```

Moving a trunk

When moving a trunk that is part of an OpenFlow member VLAN from one VLAN to another VLAN generates an error message similar to the following.

```
Trunk in use by an OpenFlow instance may not be moved.
```

Tagging/Untagging trunk

Toggling membership of the trunk from tagged to untagged when that trunk is part of an OpenFlow member VLAN generates an error message similar to the following.

```
Trunk in use by an OpenFlow instance may not be modified.
```

Enable LACP

Trying to enable LACP while OpenFlow is enabled generates the following error message.

```
LACP cannot be configured when OpenFlow is enabled.
```

Enable OpenFlow

Trying to enable OpenFlow when LACP is enabled generates the following error message.

```
OpenFlow cannot be configured when LACP is enabled.
```

Show per-flow rate limiters

Trying to show per-flow rate limiters for an instance running OpenFlow version 1.3 generates an error message similar to the following.

```
This command is supported only for an OpenFlow version 1.0
instance.
```

no allow-v1–module

Trying to run the command `[no] allow-v1-module` when OpenFlow is enabled generates an error message similar to the following.

```
V1 modules cannot be disabled when OpenFlow is enabled.
```

allow-v1–module

Trying to run the command `allow-v1-module` when OpenFlow is enabled generates an error message similar to the following.

```
V1 modules cannot be enabled when IP Control Table Mode is
enabled.
```

Non-compatible mode

Trying to enable OpenFlow when a switch is in a non-compatible mode (no allow-v1–module) generates an error message similar to the following.

```
OpenFlow cannot be enabled when V1 modules are disabled.
```

Enable virus throttling

Trying to enable virus throttling when OpenFlow is enabled generates an error message similar to the following.

```
Virus throtting cannot be enabled when OpenFlow is enabled.
```

Enable OpenFlow with virus throttling

Trying to enable OpenFlow when virus throttling is enabled generates an error message similar to the following.

```
OpenFlow cannot be configured when virus throttling is
enabled.
```

Controller error messages

Deleting an unconfigured controller

Attempt to delete a controller that has not been configured will result in an error message similar to the following.

```
HP-8206zl(vlan-3)# no openflow controller-id 2
[controller-id] 2 not found.
```

Configure or modifying an existing controller

Attempting to configure a controller that already exists or modifying the parameters of an existing controller will result in an error message similar to the following.

```
A controller is already configured with this ID.
```

Associated controllers

Attempting to delete existing controllers previously associated with an OpenFlow instance will result in an error message similar to the following.

```
Controller cannot be removed when in use by an OpenFlow
instance.
```

Setting IP Control Table mode

Attempting to set IP Control Table Mode when the switch is in compatible mode will result in an error message similar to the following.

```
IP Control Table Mode cannot be set when V1 module is
enabled.
```

Specifying and invalid flow table

Attempting to specify an invalid flow table ID will result in an error message similar to the following.

```
Invalid flow table number
```

Listen port or controller error

Commands issued from listen port or controllers are not successful.

1. Enable `debug openflow` which will display the switch output helping you to identify whether the error is occurring at the switch or the controller.
2. Enable `debug openflow instance [`*`instance-name`*`]` to further identify the error.
3. Verify the packet capture for the request and reply to isolate whether the error is occurring at the switch or the controller.

   NOTE: This problem occurs if some controllers do not fully conform to the specification and therefore cannot handle replies from the switch. The replies in the packet capture will be visible from the switch but not from the controller.

4. Enable `debug destination session` to further identify the error.

Specifying a port

If you are trying to specify an application port that is out of range will result in an error message similar to the following.

```
Invalid port. Valid range is 1024-65534.
```

Port error messages

Egress-only ports

Trying to enable or disable egress-only ports when OpenFlow is enabled generates an error message similar to the following.

```
Egress only ports can be set only when OpenFlow is disabled.
```

Limiter error messages

Removing limiters

Trying to remove a limiter when none are configured for an instance generates an error message similar to the following.

```
No limiters found for this OpenFlow instance.
```

VLAN error messages

Member to controller VLAN

Specifying a member VLAN as a controller VLAN will result in an error message similar to the following.

```
The specified VLAN is already member of OpenFlow instance
instance-name and hence cannot be added as controller
interface.
```

VLAN in an OpenFlow instance

Specifying a VLAN that is already a part of a different OpenFlow instance will result in an error message similar to the following.

```
The VLAN specified is already a member of another OpenFlow
instance.
```

More than one VLAN

Specifying more than one VLAN per instance will result in an error message similar to the following.

```
Only one VLAN can be configured as a member of an OpenFlow
instance.
```

VLAN range

Specifying a VLAN that is outside the allowed VLAN range will result in an error message similar to the following.

```
Invalid Input : VLAN-ID
```

Management VLAN

When the user tries to add the management VLAN to an OpenFlow instance will result in an error message similar to the following.

```
A management VLAN cannot be a member of an OpenFlow instance.
```

Configure VLAN as management

When the user tries to configure an OpenFlow instance VLAN as management VLAN will result in an error message similar to the following.

```
Management VLAN cannot be configured. VLAN <n> is member of
an OpenFlow instance.
```

Dynamic VLAN

When a dynamic VLAN is added as a member VLAN will result in an error message similar to the following.

```
Dynamic VLAN cannot be added as a member VLAN.
```

Controller interface

Adding a controller interface as member VLAN will result in an error message similar to the following.

```
Controller interface cannot be added as member VLAN.
```

Instance error messages

Enable a named instance

Attempting to enable a named instance without a listen port or controller and a member VLAN will display an error message similar to the following.

```
A controller and a member VLAN must be added to the named
instance before enabling it.
```

Enable an aggregate instance

Attempt to enable an aggregate instance without a listen port or controller will display an error message similar to the following.

```
A listen-port or a controller must be added to the aggregate
instance before enabling it.
```

Maximum number of instances

Configuring an instance when the maximum number of OpenFlow instances is already configured will display an error message similar to the following.

```
Maximum number of OpenFlow instances (128) already
configured.
```

Instance name that exceeds length

Configuring an instance with a name that exceeds the maximum length requirement will display an error message similar to the following.

```
Maximum length of the instance-name is 32 characters.
```

Create an aggregate instance

Trying to create an aggregate instance when a named instance already exists on the switch will display an error message similar to the following.

```
An aggregate instance cannot be created when named instances
exist.
```

Create a named instance

Trying to create a named instance when an aggregate instance is already configured will display an error message similar to the following.

```
Named instances cannot be created when an aggregate instance
exists.
```

Deleting an instance

Trying to delete a nonexistent instance will display an error message similar to the following.

```
Instance not found.
```

Enabling an instance

Attempt to enable an OpenFlow instance without configuring a listen port or a controller will display an error message similar to the following.

```
A listen-port or a controller, and a member VLAN must be
added to the named instance before enabling it.
```

Delete a member

Trying to delete a member which does not belong to the instance will display an error message similar to the following.

VLAN *VLAN-ID* is not a member of this instance.

Modifying backoff interval

Trying to modify the backoff interval when the instance is enabled will display an error message similar to the following.

```
Instance configuration cannot be modified when the instance
is enabled.
```

Instance name

When naming an instance, only alphanumeric characters, numerals and underscores are allowed in the instance name. Failure to following this rule will display an error message similar to the following.

```
Invalid name. Only alphanumeric characters and underscores
are allowed.
```

Errors concerning auxiliary connections

Removing auxiliary connection

Removing an auxiliary connection which is associated displays an error message similar to the following

```
Auxiliary connection is in use by an OpenFlow instance and
cannot be removed.
```

Deleting unconfigured auxiliary connection

Deleting an auxiliary connection that has not been configured displays an error message similar to the following.

```
Auxiliary connection index not found.
```

Associating multiple auxiliary indexes

Associating more than one auxiliary index displays an error message similar to the following.

```
Only one auxiliary connection can be configured per main
controller connection.
```

Associating un-configured auxiliary indexes

Associating an auxiliary index which is not configured displays an error message similar to the following.

```
No auxiliary connection is configured with this index.
```

Checking for the static limit

Checking for the static limit and error out while configuring displays an error message similar to the following.

```
Maximum number of auxiliary connections configured.
```

Associating auxiliary connection

Associating an auxiliary connection to an instance running version 1.0 displays an error message similar to the following.

```
Auxiliary connection can only be associated with instance
running version 1.3 and above.
```

Associating multiple auxiliary connections

Associating more than one auxiliary connection to an instance controller connection displays an error message similar to the following.

```
Only one auxiliary connection can be configured per main
controller connection.
```

Other scenarios

Setting policy engine resource usage when OpenFlow is enabled

When the policy engine resource usage is set while OpenFlow is enabled, will display an error message similar to the following.

```
Resource usage can be set only when OpenFlow is disabled.
```

Securing a connection with no certificate configured

When securing a connection with no certificate configured for OpenFlow, will display an error message similar to the following.

```
Certificate for OpenFlow is not configured.
```

Setting the protocol version with instances enabled

Setting the protocol version when instances are enabled will display a message similar to the following.

```
Instance configuration cannot be modified when the instance
is enabled.
```

Entering the wrong protocol version

Entering the wrong protocol version will display an error message similar to the following.

```
Entering the wrong protocol version will display an error
message similar to the following.
```

Troubleshooting scenarios for instances

Troubleshooting an instance

To troubleshoot instances, check the following.

- To connect a controller there must be ip-connectivity between controller and switch over the controller VLAN.
- The controller must be capable of negotiating to a version equal to or less than the configured or supported version.
- Use the `show openflow` command to check instances

Example

```
HP-Stack-3800(config)# show openflow
OpenFlow                          : Enabled
IP Control Table Mode           : Disabled

Instance Information
        No. of        No. of       OpenFlow
Instance Name           Oper.Status  H/W Flows S/W Flows  Version
----------------- ------------  --------- ---------- ----------
test              Down          0         0          1.0
```

- Use the `show openflow instance [`*`instance-name`*`]` command

Example

```
HP-Stack-3800(config)# show openflow instance test
Configured OF Version     : 1.0
Negotiated OF Version    : 1.0
Instance Name            : test
Admin. Status            : Enabled
Member List              : VLAN 3
Listen Port              : 6677
Oper. Status             : Down
Oper. Status Reason      : NA
```

```
Datapath ID              : 0003082e5f698e25
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : 0
No. of Sw Flow Tables    : NA
Egress Only Ports        : None
Table Model              : Single Table
Controller Id Connection Status Connection State Secure  Role
------------- ----------------- ---------------- ------  ------
1               Disconnected       Backoff            No      Equal
```

Commands issued from listen port or controllers are not successful

When commands issued from the listen port or the controller are not successful, the following commands can be used to isolate and troubleshoot the problem.

Syntax

`show openflow instance [`*instance-name*`] flow-table [`*table#*`] table-capabilities`

To display the table-capabilities of the instance in OpenFlow 1.3.

Syntax

`show vlan [`*member-vlan-no*`]`

To display the port-description.

Syntax

`show openflow instance [`*instance-name*`]`

To see egress-only ports.

Syntax

`show openflow instance [`*instance-name*`]port-statistics`

To display port statistics.

Syntax

`show openflow instance [`*instance-name*`] meters [`*number*`]`

To display the meter statistics.

Syntax

`show openflow instance [`*instance-name*`]groups`

To display groups.

Connection interruption mode setting

For minimal impact to an underlying network when a switch loses connection to the controller, the recommended setting is `fail-standalone` mode.

Flow modification

Add/Modify/Delete flow

When a request to add, modify or delete a flow mod is rejected by the switch, use the following command.

Syntax

```
show openflow instance [instance-name]message-statistics
```

Example

```
HP-Stack-3800(config-class)# show openflow instance test
message-statistics

OpenFlow
Message Type       Received          Rejected
 ----------------  ---------------  --------
OFPT_FLOW_MOD        0                  0
OFPT_PORT_MOD        0                  0
OFPT_GROUP_MOD       0                  0
OFPT_METER_MOD       0                  0
```

Verifying flows

The flow can be verified at the switch by using the following command.

Syntax

```
show openflow instance [instance-name]flows
```

Enable `debug openflow` at the switch. Run the command and observe the debug output for more specific rejection reasons why the flow is rejected by the switch.

NOTE: Similar troubleshooting techniques can be employed for port-modification, meter-modification and group-modification issues.

Programming flow errors

When programming flows via a controller, error messages may be returned based on implementation restrictions in the OpenFlow switch. Examples relevant to OpenFlow 1.3 include:

- Table 0 restrictions
- Table 0, a read-only table, in the OpenFLow 1.3 multiple pipeline represents the start of the pipeline.

IP control table restrictions

Error conditions for Table 50 may be caused by the following.

- Table-miss rule is read-only.
- Only unicast IP addresses can be used as match parameters in a flow.
- `Only "Goto" instruction is supported by this table.`
- `Flow with invalid VLAN match parameter is not allowed. A VLAN that does not exist on the switch is considered invalid.`

Possible errors returned to the controller:

OFPERR_OFPMFC_EPERM
OFPERR_OFPFMFC_TABLE_FULL
OFPERR_OFPBMC_BAD_FIELD (Bad or unsupported match parameter in the flow)
OFPERR_OFPBAC_BAD_TYPE (Bad or unsupported action in the flow)
OFPERR_OFPBIC_BAD_TABLE_ID
OFPERR_OFPFMFC_UNKNOWN (Any internal system error)

Policy engine table restrictions

Error conditions for Table 100, 101, or 102 may result from the following:

- In Aggregate mode, an Output-Port action is allowed only if the flow has VLAN as a match field or has as a Modify-VLAN action specified.
- Modify VLAN-PCP and P-ToS are the only Set—field actions allowed along with Output:NORMAL action.

OpenFlow v1.0 instance

OpenFlow 1.0 exposes a single table to the controller. The action of the default table-miss rule for such an instance is "`Goto Controller`".

OpenFlow 1.3 instance

OpenFlow 1.3 instance exposes a multi-table model. For every table, the action of the default table-miss rule is “DROP”. For traffic to traverse the multi-table pipeline, the table-miss rule for every table must be modified appropriately by the controller.

Example

Consider the table model in standard mode comprised of tables 0, 100, 200-201-202-203:

- If a rule is programed into table 200 that permits traffic, then unless the default “table-miss rule” for table 100 is modified, traffic will not pass to table 200.
- If the default table-miss rule of table 100 is modified with the action given as “Gototable 200”, traffic will proceed to table 200. A table-miss rule would have to be programmed similarly for table 200 and so on.

NOTE: A table-miss rule is a flow with priority of 0 and all match fields wild-carded.

Flows go missing after addition

Verify the idle-timeout/hard-timeout of the flow.

- Table 50 supports only 12 seconds as the minimum hardware refresh rate. Flows programmed in this table should have at least an idle-timeout of twice that, or 24 seconds.
- Tables 100/101/102 support a configurable hardware refresh rate. If the “policy-engine-table refresh-interval” is configured for 5 seconds, then minimum idle-timeout supported would be 10 seconds (double the time configured.)

Missing line rate performance after flows are successfully installed

If an instance is running OpenFlow v1.0 and the flow cannot be accommodated in the hardware or a higher priority overlapping rule is present in software or we have reached the policy engine usage limit configured, then . the flow will be housed in the software table. This is verified by the `show openflow instance [instance-name] flows` command.

If the flow is programmed in software, line rate performance will not be seen in packet forwarding.

To know which flows will be accommodated in hardware, see the Flow classification section of this document.

For an OpenFlow1.3 instance, there could be several software tables, 200 to 203.

OpenFlow match on TCP flags & L4 port ranges

Matching on TCP flags and TCP/UDP port ranges

TCP Flags and L4 port ranges are supported as match parameters in Flow Modification messages from the controller. Experimenter Match Fields are used to accomplish this operation.

Table 7 Matching on TCP Flags and TCP/UDP port ranges

Supported	Not supported
Match on TCP Flags and UDP/TCP source/destination port ranges in OpenFlow rules.	TCP Flags and UDP/TCP source/destination port ranges cannot be set/modified using an OpenFlow action.
Match support available for v1.3 instances only.	Instances negotiated to 1.0 will not support the feature (as 1.0 does not support Experimenter Match fields).
Match capability is available for rules in Policy Tables (TCAM) and Software Tables.	IP-Control-Table (Table-50) and MAC Table (Table 40/41) will not support matching on TCP flags or port ranges.
Matching is supported on the aforementioned tables for Instances configured in IP-Control table mode and Standard Match Mode.	Masking is not supported for port ranges.
Match masks are supported for TCP Flags.	N/A
Experimenter OXM class will be used to communicate the match capability to the controller (in TABLE_FEATURES_REPLY).	N/A
Controllers wanting to program a rule with these match parameters should use the Experimenter Flow Match Fields to specify the TCP Flags/Port range match parameters along with the experimenter ID.	N/A

Experimenter match fields

ONF assigned vendor ID will be expected in the experimenter Field for all the OpenFlow messages containing the Experimenter Match fields.

0x00002481 is the HP Vendor ID.

The following values should be used by controllers in the “oxm_field” of the Experimenter Match Fields in Flow Modification messages.

OXM field	Value
UDP Source Port Range	0
UDP Destination Port Range	1
TCP Source Port Range	2

OXM field	Value
TCP Destination Port Range	3
TCP Flags	4

Values should be encoded post the Experimenter ID field in the OXM. For TCP Flags, the value and mask will be 16-bits in length each. Similarly for Port Ranges, 16-bits will be used to encode the Range Begin value followed by 16-bits for Range End value.

Flow Mod Validations

Table 8 Flow Mod Validations

Scenario	Error Type	Error Code
The “experimenter” field in the experimenter header of flow mod message contains a value other than HP_VENDOR_ID	OFPET_BAD_MATCH	OFPBMC_UNKNOWN
The payload for the TCP flags match field contains an invalid value. (Ex: in TCAM if any bit in position 6:7 is set)	OFPET_BAD_MATCH	OFPBMC_BAD_VALUE
If either OFPXMT_OFB_TCP_SRC/ OFPXMT_OFB_UDP_SRC or OFPXMT_OFB_TCP_DST/ OFPXMT_OFB_UDP_DST is already present in the flow mod and L4 source port range or, L4 destination port range matching is also specified respectively.	OFPET_BAD_MATCH	OFPBMC_DUP_FIELD
If the port range match is specified without the OFPXMT_OFB_IP_PROTO match pre-requisite.	OFPET_BAD_MATCH	OFPBMC_BAD_PREREQ
If the TCP flag matching is specified without the IP_PROTO match being set to 6 (TCP).	OFPET_BAD_MATCH	OFPBMC_BAD_PREREQ
If all the TCAM range registers for a slot are used up, an attempt to install a new rule on the slot with L4 port range match would return OFPET_EXPERIMENTER error message to the controller. The Error code is as agreed between the Switch and the Controller team (0). The “experimenter” field will have the HP_VENDOR_ID.	OFPET_EXPERIMENTER	Exp_type = OFPERR_OFPET_EXPERIMENTER_RANGE_FULL (0)

Addition or modification of tag for single-tagged packets

This is accomplished with the action “OFPAT_SET_FIELD” and setting the field to “OFPAT_SET_VLAN_VID (Set the 802.1q VLAN id)” inside the packet.

OFPAT_PUSH_VLAN and OFPAT_POP_VLAN are supported for single tagged packets only.

Is	Is not
Support for OFPAT_PUSH_VLAN and OFPAT_POP_VLAN on all OpenFlow instance pipeline models.	OFPAT_PUSH_VLAN and OFPAT_POP_VLAN action will not be supported on v1 mode of operation.
Support for OFPAT_PUSH_VLAN and OFPAT_POP_VLAN on v2 and v3 modes of operation.	OFPAT_PUSH_VLAN action does not support double tagging.
Support for OFPAT_PUSH_VLAN only with ether-type as 0x8100 (802.1q)	OFPAT_PUSH_VLAN and OFPAT_SET_FIELD of OFP_VLAN_VID actions will not be supported in the same flow.
OFPAT_PUSH_VLAN action on an already tagged packet does not add a fresh 802.1q tag. It will modify the existing 802.1q tag in the packet.	
OFPAT_POP_VLAN action will only strip the 802.1q tag in the packet.	

Troubleshooting scenarios and error messages

How to troubleshoot if instance is not coming up

When an instance is not coming up, use the following commands to troubleshoot the instance status.

1. Run the command `HP-Stack-3800(config)# show openflow`

```
HP-Stack-3800(config)# show openflow
OpenFlow                    : Enabled
IP Control Table Mode       : Disabled
Instance Information
                    No. of       No. of       OpenFlow
Instance Name                          Oper. Status  H/W Flows   S/W Flows   Version
-------------------------------- ------------  ----------  ----------  --------
 test                                  Down     0             0            1.0
```

2. Run the command `HP-Stack-3800(config)# show openflowinstance test`

```
HP-Stack-3800(config)# show openflowinstance test
Configured OF Version     : 1.0
Negotiated OF Version    : 1.0
Instance Name            : test
Admin. Status            : Enabled
Member List              : VLAN 3
Listen Port              : 6677
Oper. Status             : Down
Oper. Status Reason      : NA
Datapath ID              : 0003082e5f698e25
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : 0
No. of Sw Flow Tables    : NA
Egress Only Ports        : None
Table Model              : Single Table

Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1               Disconnected        Backoff            No     Equal
```

Reporting problems

If you are unable to solve a problem with OpenFlow, do the following:

1. Read the release notes for OpenFlow to see if the problem is known. If it is, follow the solution offered to solve the problem.
2. Determine whether the product is still under warranty or whether your company purchased support services for the product. Your operations manager can supply you with the necessary information.
3. Access **HP Support Center** and search the technical knowledge databases to determine if the problem you are experiencing has already been reported. The type of documentation and resources you have access to depend on your level of entitlement.

   NOTE: The HP Support Center at **HP Support Center** offers peer-to-peer support to solve problems and is free to users after registration.

   If this is a new problem or if you need additional help, log your problem with the HP Support Center, either on line through the support case manager at **HP Support Center**, or by calling HP Support. If your warranty has expired or if you do not have a valid support contract for your product, you can still obtain support services for a fee, based on the amount of time and material required to solve your problem.
4. If you are requested to supply any information pertaining to the problem, gather the necessary information and submit it. The following sections describe some of the information that you may be asked to submit.

9 Support and other resources

Contacting HP

Before you contact HP

Be sure to have the following information available before you call contact HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error message
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) website at **http://welcome.hp.com/country/us/en/wwcontact.html**.

For HP technical support:

- In the United States, for contact options see the Contact HP United States website at **http://www8.hp.com/us/en/home.html**.

  To contact HP by phone:

  - Call 1-800-HP-INVENT (1-800-474-6836.) This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, see the HP website at **http://www.hp.com/hps**.
  - In other locations, see the Contact HP worldwide (in English) website at **http://www8.hp.com/us/en/contact-hp/contact.html**.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website at **http://www.hp.com/country/us/en/contact_us.html**. After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Documents

You can find additional switch documents by using the Manuals page of the HP Business Support Center website at **http://pro-networking-h17007.external.hp.com/us/en/support/converter/index.aspx**.

Additional documentation for your HP Switch may include:

- *Access Security Guide*
- *Advanced Traffic Management Guide*

- *Basic Operation Guide*
- *IPv6 Configuration Guide*
- *Management and Configuration Guide*
- *Multicast and Routing Guide*
- *Event Log Message Reference Guide*
- *Comware CLI Commands in ProVision Software*

Websites

HP product websites are available for additional information.

- HP Switch Networking web site: **http://www.hp.com/networking/support**
- HP Technical Support website: **http://www.hp.com/support**

Typographic conventions

This document uses the following typographical conventions:

`%`, `$`, or `#`	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells. A number sign represents the superuser prompt.
audit(5)	A manpage. The manpage name is *audit*, and it is located in Section 5.
`Command`	A command name or qualified command phrase.
`Computer output`	Text displayed by the computer.
Ctrl+x	A key sequence. A sequence such as **Ctrl+x** indicates that you must hold down the key labeled **Ctrl** while you press another key or mouse button.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
ERROR NAME	The name of an error, usually returned in the `errno` variable.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	The defined use of an important word or phrase.
`User input`	Commands and other text that you type.
`Variable`	The name of a placeholder in a command, function, or other syntax display that you replace with an actual value.
[ ]	The contents are optional in syntax. If the contents are a list separated by |, you must choose one of the items.
{ }	The contents are required in syntax. If the contents are a list separated by |, you must choose one of the items.
...	The preceding element can be repeated an arbitrary number of times.
□	Indicates the continuation of a code example.
|	Separates items in a list of choices.
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.

CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

Customer self repair

HP products are designed with many Customer Self Repair parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period HP (or HP service providers or service partners) identifies that the repair can be accomplished by the use of a Customer Self Repair part, HP will ship that part directly to you for replacement. There are two categories of Customer Self Repair parts:

- Mandatory—Parts for which Customer Self Repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service.
- Optional—Parts for which Customer Self Repair is optional. These parts are also designed for customer self repair. If, however, you require that HP replace them for you, there may or may not be additional charges, depending on the type of warranty service designated for your product.

NOTE: Some HP parts are not designed for Customer Self Repair. In order to satisfy the customer warranty, HP requires that an authorized service provider replace the part. These parts are identified as *No* in the Illustrated Parts Catalog.

Based on availability and where geography permits, Customer Self Repair parts will be shipped for next business day delivery. Same day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the telephone. HP specifies in the materials shipped with a replacement Customer Self Repair part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a Customer Self Repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.

For more information about the HP Customer Self Repair program, contact your local service provider. For the North American program, visit the HP website at **http://www.hp.com/go/selfrepair**.

10 Documentation feedback

HP 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@hp.com**.) Include the document title and part number, version number, or the URL when submitting your feedback.

NOTE: There has been a change to the style of the documentation with the newest release. The “Command Table” commonly seen at the beginning of the chapters has been replaced with the ability to search for commands using the index. All commands are now listed in the index within the category “Command syntax”.

A Flow classification on v1, v2 and v3 modules

Hardware differences between v1, v2 and v3 modules affect flow match and capabilities.

For additional information about modules, see the latest Release Notes for your switch.

and the *HP 8200 zl, 5400 zl, 3500, and 6200 yl Switch Series Technical Overview White Paper*, 4AA0-5388ENW.pdf available on the HP Switch Networking web site at **http://www.hp.com/networking/support**.

Hardware match chart

Figure 16 Standard match model — v1

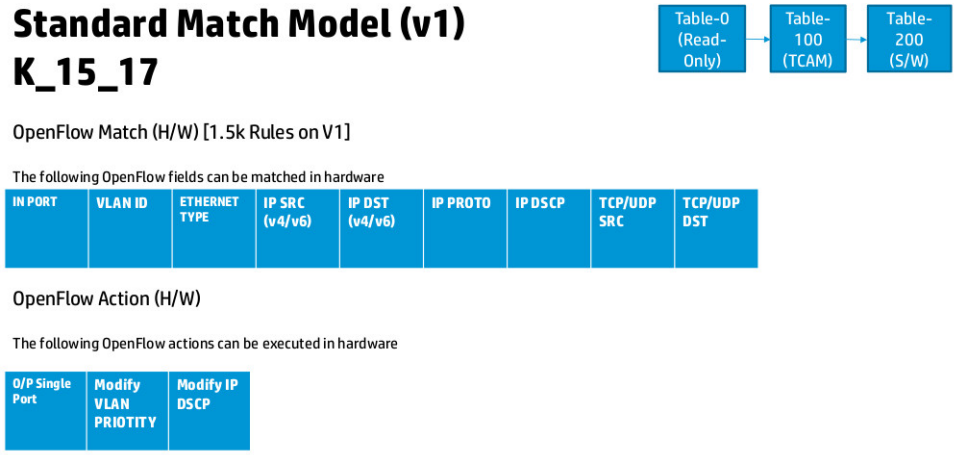


Figure 17 Standard match model — v2 &v3

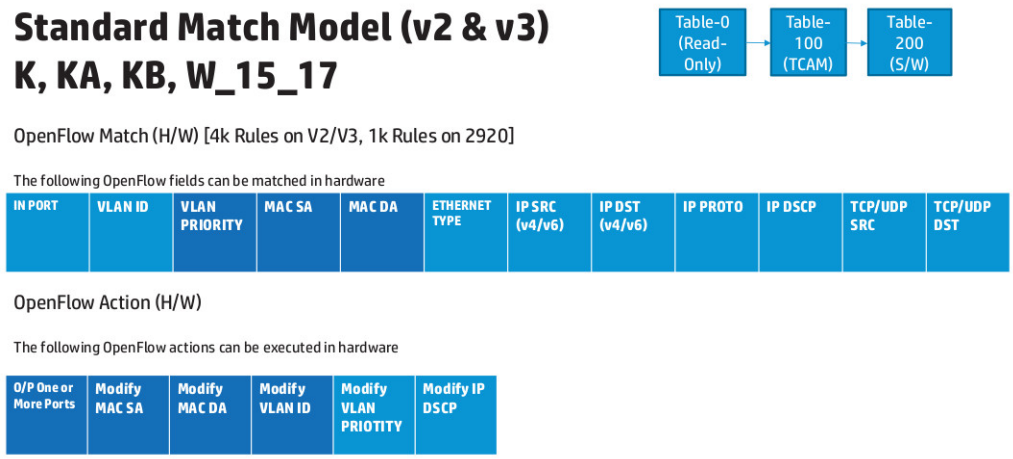


Figure 18 Custom pipeline model — v3

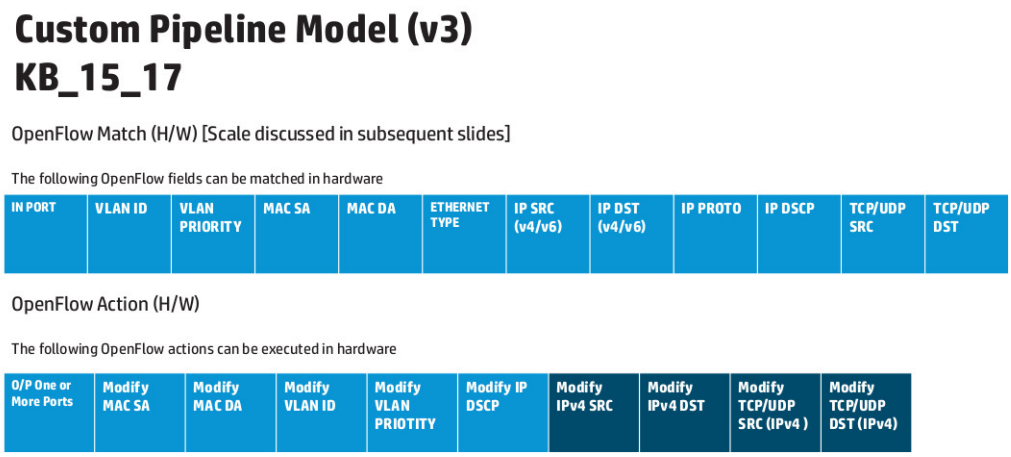


Figure 19 Custom pipeline model — default pipeline

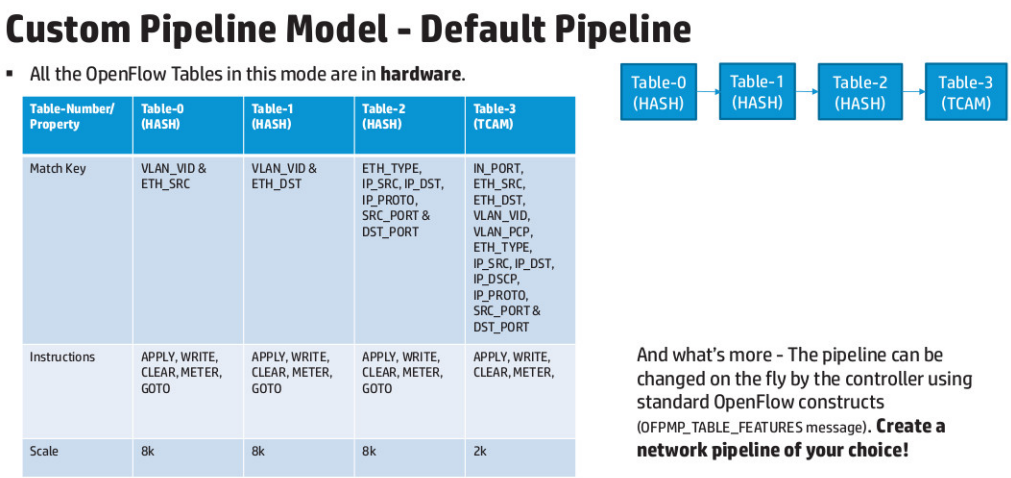
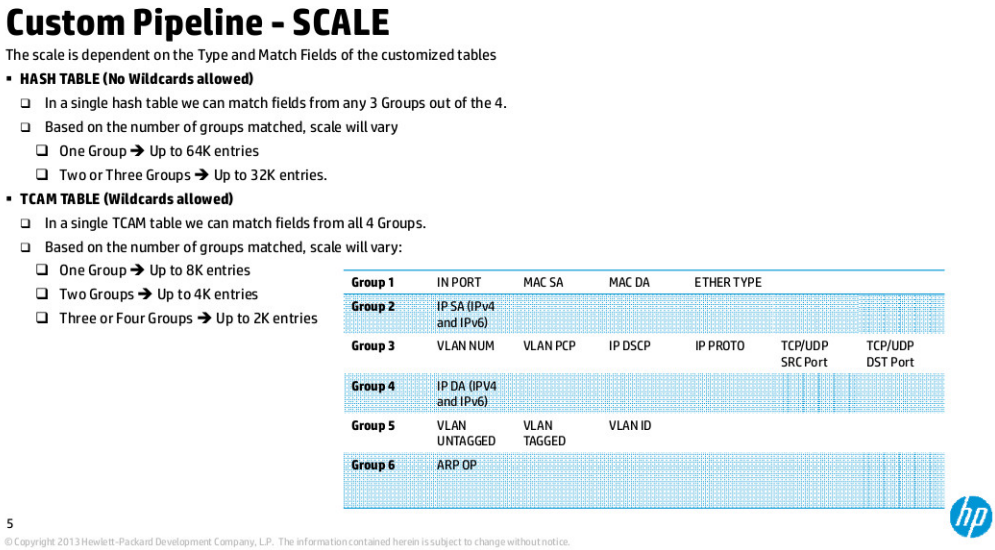


Figure 20 Custom pipeline scale



OpenFlow 1.3 multi-table model and device modes

Figure 21 Standard mode (default)

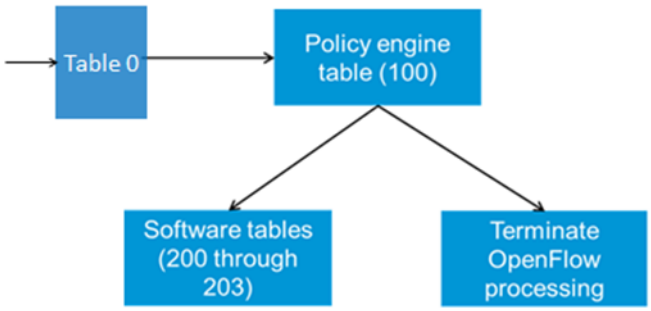


Figure 22 IP control table mode

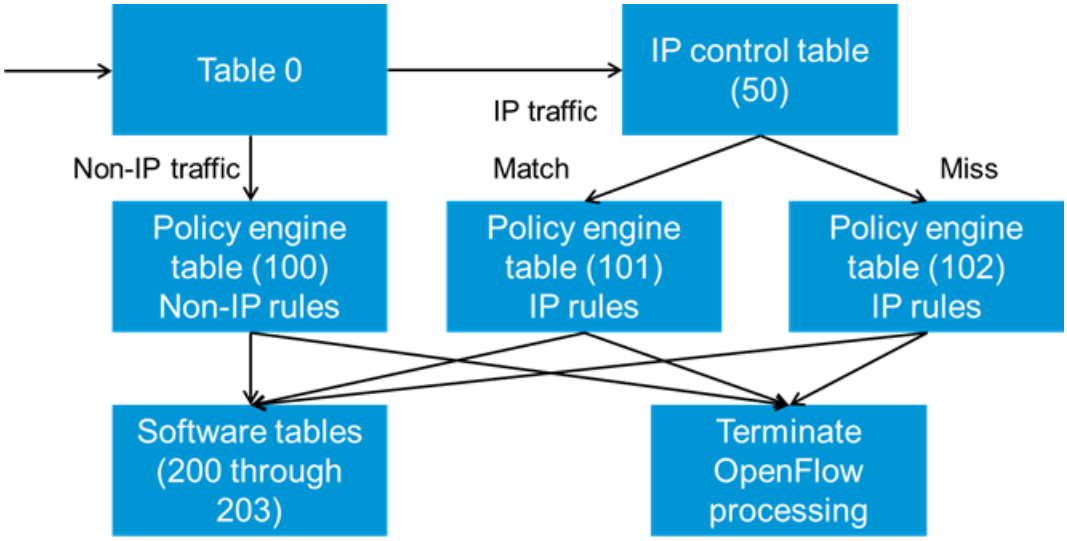


Table 9 Device modes and OpenFlow table model

Openflow Protocol Version	**Switch Mode**	**Table Model**	**Number of tables**	**Matching ability**	**Actions in Hardware (Nov 2013)**
V1.0	Compatible Mode – "allow-v1-modules" (V1 and V2) acts as V1	Single table only	1	Same as 15_10	Same as 15_10
V1.0	Non Compatible Mode – "no allow-v1-modules" (V2 only) act as V2	Single table only	1	Full 12 tuple match in policy engine	Same as 15_10 Plus new actions – rewrite VLAN ID, rewrite MAC address, forward to multiple ports
V1.3	Compatible Mode (V1 and V2) acts as V1	Standard Match	1 policy engine + 1 software	Same as 15_10	Same as 15_10
V1.3	Non-Compatible Mode (V2 only) act as V2	Standard Match	1 policy engine + 1 software	Full 12 tuple match in policy engine	Same as 15_10 Plus new actions - rewrite VLAN ID, rewrite MAC address, forward to multiple ports
V1.3	Non-Compatible Mode (V2 only) act as V2	IP Control Mode	1 IP control table + 3 policy engine tables (IP control table match, IP control table miss, Non-IP)+1 software	{src. VLAN, src. IP, dst. IP} in IP control table + Full 12 tuple match in policy engine	Same as 15_10 Plus new actions in - rewrite VLAN ID, rewrite MAC address, forward to multiple ports

B Implementation notes

This section documents some of the behaviors exhibited during the implementation of OpenFlow. These behaviors were exposed during testing and may include unit, conformance, integration, interoperability, stress and system testing.

A hardware flow with an idle timeout of 10 seconds gets deleted even though packets match the flow within the idle timeout

Problem statement

A hardware rule is programmed with idle timeout as 10 seconds and hard timeout as 0. Packets are pumped at 1000 pps to the switch matching the flow. However, after 10 seconds, the rule gets removed from the switch.

Reason for this behavior

By default the hardware statistics refresh rate (set using `openflow hardware statistics refresh rate` and information available through `show openflow`) is 20 seconds. This means that the packet count statistics get updated only every 20 seconds. So, when the idle timeout is set to less than 20 seconds, when a check is done for flow statistics after 10 seconds, it would not be updated. Hence, the flow would get deleted.

Customer Note

The user has the option of reducing or incriminating the refresh rate. However, the user needs to be aware of its implications. An increase in refresh rate would lead to deletion of flows which has an idle timeout less than the configured refresh rate. A decrease in refresh rate would lead to over-use of CPU (because of polling hardware statistics more frequently.)

Controller flows — flow in hardware and processing software

Flows with an action to send matching traffic to controller are actually installed on hardware. But, the actual traffic forwarding takes place in software as we need to add the required OpenFlow specific headers. Due to this characteristic, the actual forwarding will not take place at the line rate. A sample controller flow would look like:

Example

In this example, any packet that comes on port A1, will be forwarded to the controller after adding required OpenFlow packet headers (as the packet will be sent as a packet_in) to the controller. Since this processing is done on software, we will not be able to send the incoming traffic at line rate.

```
HP-8206zl(openflow)# show openflow instance test flows
Flow 1
  Incoming Port   : A1              Ethernet Type      : 0x0000
  Source MAC      : 000000-000000   Destination MAC     :
000000-000000
  VLAN ID         : 0               VLAN priority       :
  Source IP       : 0.0.0.0         Destination IP      : 0.0.0.0
  IP Protocol       : 0               IP ToS Bits         : 0
  Source Port     : 0               Destination Port    : 0
  Priority        : 2
  Duration        : 1 seconds
  Idle Timeout    : 60 seconds      Hard Timeout       : 0 seconds

  Packet Count    : 1               Byte Count          : 0
  Flow Location   : Hardware
```

```
Actions
  Controller Port
```

DUT matches and processes incoming untagged packets for VLAN id

For certain flows with a match on the VLAN ID, even untagged packets are matched. This happens on untagged ports only. The existing behavior exists because L2 hardware adds the VLAN id and VLAN priority meta-information irrespective of whether the packet came in tagged or untagged. Flows which can be accelerated into hardware are put into hardware whereas flows which cannot be accelerated in hardware are put into software. The observed behavior is observed for hardware and software flows.

Events that change the Operational Status of the OpenFlow instance

The `Oper. Status` field indicates the operational status of the instance and can be either up or down. The operational status will be down when either the member VLAN of the OpenFlow instance does not exist on the switch or the controller VLAN of the OpenFlow instance does not exist on the switch. In the case when multiple controllers connect over multiple controller VLANs, the operational status will be down when none of the controller VLANs exist on the switch. When the member VLAN is down - all ports on the member VLAN are down.

For example, the `show openflow instance` displays all the OpenFlow instance related information as follows:

```
show openflow instance <test>
```

NOTE: Note that for purposes of this example the instance *<test>* has been created.

```
Instance Name            : Test
Admin. Status            : Enabled
Member List              : VLAN 3
Listen Port              : 6633
Oper. Status             : Down
Datapath ID              : 00030026f1212000
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds

Controller Id Connection Status Connection State
------------- ----------------- ----------------
2             Disconnected      Backoff
```

OpenFlow's influence on CPU generated packets

In some cases, the CPU generated packets will be effected by the TCAM rules. This behavior is consistent with OpenFlow versions 1.0 and 1.3. One example of such a case is when a rule is in place with the `in_port`as a wild-card but has a SRC IP address that matches the IP address configured on the switch.

OpenFlow 1.0 supports IP address masking

OpenFlow supports IP subnet mask. Controllers can specify the subnet mask associated with an IP address and sent to the OpenFlow switch. The switch accepts the IP address with the subnet mask and associates any packets coming with the subnet mask with the rule.

For example the K.15.10. OpenFlow implementation supports the ability to match on IP address and subnet mask when the OpenFlow controller programs such flows. Consider this example where the ovs-ofctl utility is used to add a flow that matches on a network source address of 1.1.1.1 with a subnet mask of /24. Note that 10.10.10.1 here is the IP address of the switch which has an OpenFlow listen port open on port 6633.

```
openflow@openflow-ubuntu-08:~$ ovs-ofctl add-flow
tcp:10.10.0.1:6633 ip,nw_src=1.1.1.1/24,actions=output:1
```

To verify that this flow has been installed on the switch, we run the `ovs-ofctl` command and verify the output.

```
openflow@openflow-ubuntu-08:~$ ovs-ofctl dump-flows tcp:10.10.0.1:6633
NXST_FLOW reply (xid=0x4): cookie=0x0, duration=13.535s, table=0,
n_packets=0, n_bytes=0, ip,nw_src=1.1.0.0/24 actions=output:1
```

The `show openflow instance t1 flows` command when executed on the HP switch displays the following:

Example

```
HP-3500yl-48G-PoEP(of-inst-t1)# show openflow instance t1
Configured OF Version    : 1.3
Negotiated OF Version    : 1.3
Instance Name            : t1
Admin. Status            : Enabled
Member List              : VLAN 3
Listen Port              : None
Oper. Status             : Up
Oper. Status Reason      : NA
Datapath ID              : 0003b499ba86bf80
Mode                     : Active
Flow Location            : Hardware and Software
No. of Hw Flows          : 0
No. of Sw Flows          : 0
Hw. Rate Limit           : 0 kbps
Sw. Rate Limit           : 100 pps
Conn. Interrupt Mode     : Fail-Secure
Maximum Backoff Interval : 60 seconds
Probe Interval           : 10 seconds
Hw. Table Miss Count     : NA
No. of Sw Flow Tables    : 1
Egress Only Ports        : None
Table Model              : Policy Engine and Software

Controller Id Connection Status Connection State Secure Role
------------- ----------------- ---------------- ------ ------
1             Connected         Active           Yes    Equal
```

Virtualization mode verses Aggregation mode — VLAN tags in `packet_in` messages

There is a difference in the `packet_in` messages that are sent to the OpenFlow controller by the switch based on the mode that the OpenFlow instance is operating in. In Virtualization mode , no VLAN tags are sent in `packet_in` messages sent to the OpenFlow controller. Even if the packets that came in to the switch on the OpenFlow instance had VLAN tags, they will get removed by the switch in `packet_in` messages sent to the controller. Flows that match on VLAN PCP or modify VLAN PCP are not supported in Virtualization mode. Any tagged packets that are received in Virtualization mode may have their PCP modified to default. VLAN PCP isn't matched because tag is always stripped in Virtualization mode.

In Aggregate mode, VLAN tags are always sent by the switch in `packet_in` messages sent to the OpenFlow controller. Even if the packets that came in to the switch on the OpenFlow instance did not have VLAN tags, they will be added by the switch in `packet_in` messages sent to the controller. The switch adds a VLAN tag either based on the tag that the packet already carried when it came in to the switch or based on the membership of the port that the packet came in to the switch.

Precedence level in meters

As per the OpenFlow specification 1.3.1, the prec_level given in the ofp_meter_band_dscp_remark indicates by what amount the DSCP value in the packets should be incremented if the packets exceed the band. However, the switch implementation directly replaces the DSCP value in the IP packets with the prec_level when the band exceeds the meter defined by the controller

Support for miss_len field in ‘switch configuration’ messages

The switch implementation does not honor the miss_len miss_send_len field specified in the packet-in switch configuration messages. This is because, switch doesn’t buffer packets. Due to this controller will see the entire packet copied in packet-in message with buffer_id set as OFP_NO_BUFFER.

Once a controller deletes flows from Table 0, it has to re-add in order for traffic to flow through an OpenFlow switch

OpenFlow instance running Standard-Match Mode

- When the OpenFlow instance is configured with version 1.3, as soon as the controller connects and negotiates to 1.3, the switch internally adds the following Rule 1 on Table 0 (which says: GoTo Table 100):
    - Until the K/KA.15.15 release, if the controller were to delete Rule 1, there was no impact on packet forwarding on the switch for packets coming on OpenFlow VLAN(s). Also, the switch always rejected any attempts made by the controller to add back this default rule to Table 0.
    - Starting with the K/KA.15.16 release, if the controller were to delete Rule 1, there is an impact on packet forwarding on the switch for packets coming on OpenFlow VLAN(s). Packets incoming on OpenFlow VLAN(s) are dropped by the switch. This continues until the controller adds the default rule back to Table 0. The switch complies to flow-mod requests from the controller on Table 0 based on its advertised capabilities.

OpenFlow instance running IP-Control Mode

- Rules on Table 0 in this mode:
    - Rule 1 -> All fields are wildcarded on Table 0 (which says Goto 100).
    - Rule 2 -> Match on Ether-Type IPv4 on Table 0 (that says Goto 50).
    - Rule 3 -> Match on Ether-Type IPv6 on Table 0 (that says Goto 50).
- Starting with the K/KA.15.16 release:
    - If Rule 1 is deleted, all non-IP traffic is dropped incoming on OpenFlow VLAN(s).
    - If Rule 2 is deleted, all IPv4 traffic incoming on OpenFlow VLAN(s) is dropped by the switch.
    - If Rule 3 is deleted, all IPv6 traffic incoming on OpenFlow VLAN(s) is dropped by the switch.

- There is also the case of a Table Miss Rule on Table 50:
  - Rule 4 -> All fields are wildcarded on Table 50 (which says Goto 102).
- Starting with the K/KA.15.16 release:
  - If Rule 4 is deleted, all IP (both IPv4 & IPv6) traffic that doesn't match any of the rules on Table 50 is dropped by the switch.
- In all the above cases, the controller has to add these rules back to get the traffic to be forwarded as desired.

OpenFlow custom pipeline implementation notes

- OpenFlow Table modifications cannot be done in v1/v2 modules or on v3 modules in compatibility mode.
- When the instance is configured in Standard match mode or ip-control-table-mode, controllers cannot change the default pipeline advertised by controller.
- For IPv6 packets, MAC SA modification would not be allowed. L4 ports modifications won't be allowed for IPv6 packets.
- Write-metadata instructions are not supported.
- Rules with actions as packet-modifications and OFPP_CONTROLLER would be directly rejected. However, if the rules spans across multiple tables (write-instruction in first table having packet modifications & write-instructions in further tables having OFPP_CONTROLLER) would be accepted – however, the packets taken to CPU/CONTROLLER would be unmodified.
- Special ports OFPP_ALL, OFPP_LOCAL, OFPP_TABLE, and OFPP_IN_PORT are not supported.
- Write-instruction having OFPP_CONTROLLER cannot have a Goto instruction associated with it.
- Write-instruction rules should always have output port specified or Goto to next table or "output port + goto".
- Counters are associated with tables and flow entries if available. Else the table or flow creation would be rejected with an error `Resources not available` to the controller.
- Tables configured from the controller should have a minimum size of 512 entries or the table creation request will be rejected.
- Before a table is deleted, the controller should remove all flows in previous tables pointing to the deleted table. If all flows are not removed, the controller table modification (deletion/modification) will not be allowed.
- For multiple custom-pipeline instances, the user should reduce the size of the tables in the first custom-pipeline instance. Following this procedure, the user must disable and enable the other custom-match instances for them to become operational.

NOTE: When a same OpenFlow meter is used two or more times in an OpenFlow pipeline, it will result in skewed meter rates leading to unpredictable behavior in how the packets are metered. HP recommends to not use a meter more than once in a packet pipeline to avoid undesired behaviors.

Multi-VLAN implementation notes

- For a Multi-VLAN instance, the first VLAN in the Multi-VLAN instance would be part of the DPID. Since VLANs cannot be part of multiple instances this ensures a unique DPID for each instance.
- A VLAN, which is member VLAN of one instance cannot be member VLAN of another instance.

- A VLAN cannot be dynamically added to an instance when it is enabled, the instance needs to be disabled before adding a VLAN to an OpenFlow instance.
- The user can configure VLANs which are member VLANs of an instance after creating and enabling the Multi-VLAN instance.
- At least one Member-VLAN of a Multi-VLAN instance must be configured on the switch else the `operStatus` is marked `DOWN`.
- Management and controller VLANs cannot be part of an instance.

Implementation notes for OpenFlow groups in hardware

- Groups are not support in hardware when switch is running in v1 mode.
- Special ports OFPP_ALL, OFPP_NORMAL, OFPP_TABLE, OFPP_IN_PORT, OFPP_LOCAL and OFPP_CONTROLLER would not be supported in OpenFlow groups in hardware.
- Tunnels cannot be part of OpenFlow ALL group.
- Rules in OpenFlow software tables can refer to Groups in software or hardware.
- Rules in OpenFlow hardware tables cannot refer to groups in software.
- On custom pipeline instances, groups in hardware would have counters subject to the availability of the counters.
- If the group is in software, it can only be referenced from software table.
- Rules in hardware tables with group action should NOT have a goto instruction associated with it.
- Group Modifications:
    - Modification of a group in hardware which leads to having NO Ports would NOT be allowed.
    - Group modification requests for Groups in H/W will be rejected if the resultant modification can no longer be accommodated in H/W
- In “custom mode” the groups would always be in hardware. Attempts to add groups with actions other than output ports would be rejected.
- The number of OpenFlow groups that can be created on an OpenFlow instance is 1024.

C Configuring secure connection HP VAN SDN controller

HP Switches running OpenFlow can securely connect to HP VAN SDN controller.

Follow the procedures to accomplish the secure connection.

1. On the HP Switch running OpenFlow, create a **crypto profile**.

   ### Syntax

   ```
   crypto pki ta-profile VanProfile
   ```

2. Copy root certificate to the HP switch using this command:

   ### Syntax

   ```
   copy tftp ta-certificate VanProfile [103.0.11.34] HpRoot.pem
   ```

3. Create an identity profile on the HP switch using this command:

   ### Syntax

   ```
   crypto pki identity-profile VanIdentity subject [common-name]
   ```

4. Make a certificate signing request.

   ### Syntax

   ```
   crypto pki create-csr certificate-name Vancert ta-profile
   VanProfile usage openflow
   ```

5. Copy the CSR request text in step 4 and paste to a file named “switch.csr”
6. Execute the command:

   ### Syntax

   ```
   ./signCSR.pl-in switch.csr-out switch-l 2
   ```

7. Execute the command:

   ### Syntax

   ```
   crypto pki install signed certificate
   ```

8. Copy and paste the contents of switch.pem into the HP switch console.
9. Configure OpenFlow to connect to the VAN SDN controller.

```
openflow
controller id 3 ip 103.0.11.31 port 6634 controller interface
vlan 1 instance "van"
member vlan 100
controller id 3 secure
version 1.3
limit hardware rate 10000000
limit software rate 10000
enable
exit
enable
```

D Service Insertion

NOTE: Service insertion is supported on the following switches:

HP 2920 Switch
HP 3800 Switch
HP 5400 Switch
HP 5400R Switch
HP 8200 Switch

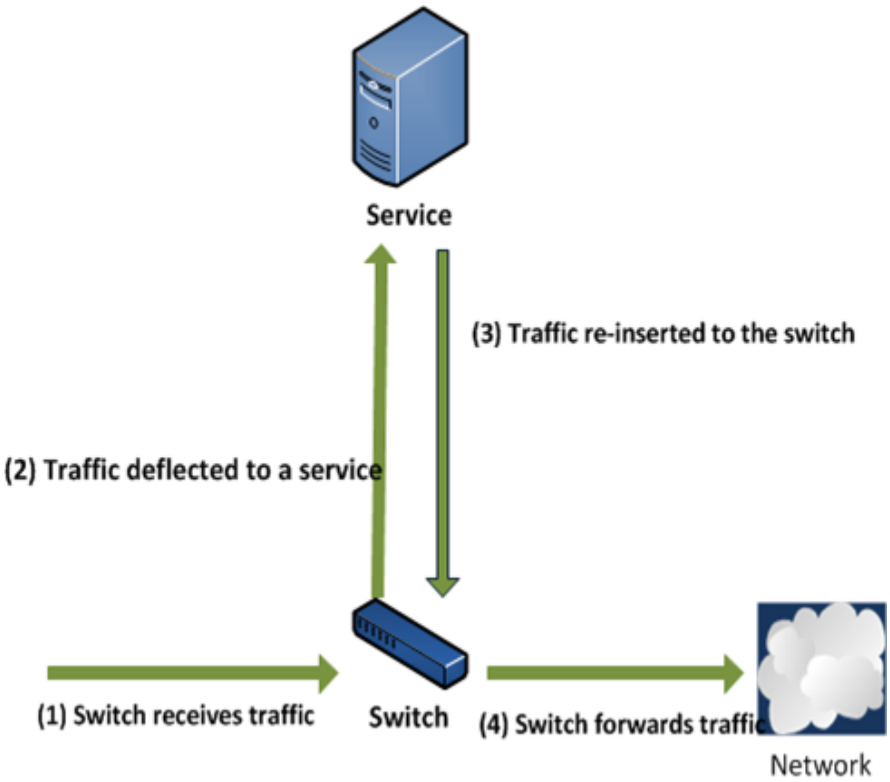
Service Insertion is not supported in v1-compatible mode.

Service Insertion is transparently inserting an external service into a traffic flow or into the traffic processing pipeline.

- Flows are re-directed to a service for inspection and then re-injected to the forwarding pipeline.
- Possible services include IPS, HP Network Protector SDN Application, Web filtering, and traffic analyzers.

Service Insertion is handled by the ASIC via a tunnel or Fast Path, and does not incur any CPU processing overhead.

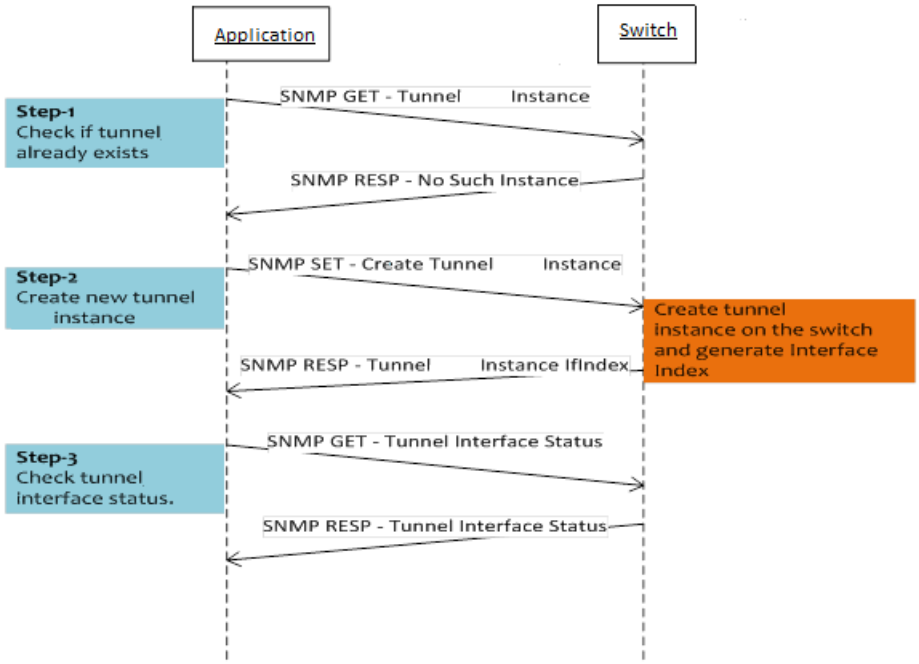
Figure 23 Inspection Service



OpenFlow and Service Tunnels

The HP switch notifies the OpenFlow controller of tunnel interface status changes (UP/DOWN). Once the controller has been notified of the tunnel instance via the OpenFlow switch agent, it can then use that tunnel as a valid output port for FLOW-MOD messages being pushed to the switch. If the OpenFlow outport action for a flow rule points to a tunnel's virtual port, the packets matching that flow rule are rerouted to the controller via the tunnel interface.

Figure 24 Integration with OpenFlow



For complete information about creating and configuring tunnels with the OpenFlow controller, see the *HP Service Insertion Guide* for your switch.

Index

Symbols

6in4 tunnels, 11
802.1X, 13

A

ACLs, 13
Active mode, 18
Administrative methods, 11
Aggregation mode, 9
Applicable HP switches, 1
Associate instance to controller, 21

B

Backoff interval, 24
Backup configuration, 31
BGP, 13
BPDU guard, 14

C

Command syntax, 107
  auxiliary-connection, 22
  auxiliary-connections, 63
  controller-id, 24
  copy tftp, 107
  crypto pki, 107
  debug, 78
  debug commands, 78
  egress-only-ports, 29
  enable/disable, 17
  hardware statistics refresh rate, 31
  hardware-statistics refresh-interval, 74
  instance, 16, 17
  instance capabilities, 65
  instance limiters, 64
  instance message statistics, 65
  instance-name, 24
  instance-name aggregate, 17, 18
  ip-ctrl-table-usuage, 30
  max-backoff-interval, 24
  member vlan , 43
  meters, 63
  multiport-filter-limit, 64
  openFlow, 16
  openflow ins *<instance name>* `src-mac-grp-table`, 35
  OpenFlow instance
    hardware rate limiting, 30
    software rate limiting, 30
  openflow instance *<instance name>* aggregate
    controller id, 21
  openflow instance *<instance name>* `dest-mac-grp-table`, 37
  openflow instance <instance-name>, 32
  openflow instance *<instance-name>* aggregate, 19
  openFlow instance *<instance-name>* member vlan, 18
  pipeline-model
    custom, 32
    ip-control, 32
    standard-match, 32
  policy-engine-usage, 30
  port statistics, 64
  show
    auxiliary-connections, 63
    instance, 26, 27, 63, 64, 65, 86, 87
    multiport-filter-limit, 64
    vlan, 86
  show openflow
    auxiliary-connections, 49
    controllers, 49
    flows, 49
    instance , 49
    port-statistics, 49
    resources, 49
  show openflow controllers , 58
  show openflow flow-table, 58
  show openflow inst, 52
  show openflow instance, 55, 63, 87
    aggregate, 59, 61
    aggregate groups, 56
    flow-table, 58, 59
    groups , 61
    instance-name, 61
  show openflow resources, 56
Configuration backup, 31
Configuration overview, 16
Configure instances, 17, 18
Configure ports, 31
Configure VLANs
  VLAN, 31
Connection interruption, 86
Controller
  errors, 80
Controllers
  show, 58
Custom pipeline
  implementation notes, 105
  overview, 67

D

Default pipeline
  custom mode, 68
Delete OpenFlow configurations, 17
Destination-ip, 52
Destination-mac, 52
Destination-port, 52
DHCP snooping, 13
DHCPv4
  client, 13
  relay, 13
DHCPv6
  client, 13
  relay, 14
Disable OpenFlow, 16

Distributed Trunking, 14
DNS, 13
Documentation
  HP website, 93
documentation
  providing feedback on, 96
DT, 14
Dynamic ARP Protection, 14
Dynamic IP Lockdown, 14

E
Enable OpenFlow, 16
Error messages, 78
Errors
  controller, 88
Ether-type, 52
Experimenter match fields
  OXM field, 89

F
Flow
  missing, 88
  missing line rate performance, 89
Flow location, 18
Flow Mod
  Validations, 90
Flow mod
  add/modify/delete, 87
Flow-type, 49

G
GVRP, 14

H
Hardware flows, 18
Hardware rate limiting, 30

I
IDM, 13
IGMP
  Proxy, 14
IGMPv2, 14
IGMPv3, 14
Implementation notes
  CPU generated packets, 102
  IP address masking, 102
  Operation Status, 102
  tagged/untagged packets, 102
  Virtualization mode, 103
In-port command, 102
Instance
  errors, 83
  members, 18
Instance to controller association, 21
Instances, 17
Interoperability, 13
  802.1X, 13
  ACLs, 13
  BGP, 13
  BPDU guard, 14
  DHCP snooping, 13
  DHCPv4 client, 13
  DHCPv4 relay, 13
  DHCPv6 client, 13
  DHCPv6 relay, 14
  Distributed Trunking, 14
  DNS, 13
  Dynamic ARP Protection, 14
  Dynamic IP Lockdown, 14
  GVRP, 14
  IDM, 13
  IGMP Proxy, 14
  IGMPv2, 14
  IGMPv3, 14
  LACP, 14
  Loop Protect, 14
  MAC Auth, 13
  MAC Lockdown, 13
  MAC Lockout, 13
  management VLAN, 13
  meshing, 13
  MLDv1, 14
  MLDv2, 14
  MSTP, 14
  OSPFv2, 14
  OSPFv3, 14
  PIM-DM, 14
  PIM-SM, 14
  Ping, 13
  Port Security, 13
  PVST, 14
  Q-in-Q, 13
  Rate limiting, 13
  remote mirror endpoint, 13
  RIP, 14
  RSTP, 14
  sFlow, 14
  SNTP, 13
  Static Multicast Routes, 14
  Static Routes, 14
  STP, 14
  STP loop guard, 14
  Telnet client and server, 13
  TFTP, 13
  TimeP, 13
  Traceroute, 13
  transparent mode, 13
  UDLD, 14
  UDP broadcast forwarder, 13
  Virus Throttling, 14
  VRRP, 14
  Web Auth, 13
Interoperability errors, 78
IP addressing masking, 102
IP control table
  restrictions, 87
IP control table pipeline
  ip match policy table

ip miss policy table, 34
L3 ignore, 34
L3 match
L3 miss, 34
non-ip policy table, 34
IP Fragments, 12
IP-protocol, 52
IP-TOS-BITS, 52
IPv6, 11

L

LACP, 14
Listener ports, 20
Loop Protect, 14

M

MAC auth, 13
MAC group table
source MAC group
destination MAC group, 33
MAC group tables
metadata
metadata_mask, 34
MAC groups
MAC CAM, 33
standard match
ip control mode, 33
MAC Lockdown, 13
MAC lockout, 13
Management VLAN, 13
Maximum OpenFlow instances, 16
Meshing, 13, 78
Meter information
Meter for specific instance, 63
MLDv1, 14
MLDv2, 14
MSTP, 14

O

OFPP TABLE action, 12
OpenFlow
architecture, 8
command context, 16
delete, 17
disable, 16
enable, 16
features, 10
foundation website, 8
instance mode, 18
instance-name, 16
maximum instances, 16
RFCs, 12
standards, 12
switch specification version, 8
OpenFlow and service tunnels, 108
OpenFlow configuration
Introduction, 7
OpenFlow Multi-VLAN instance
Overview, 43
Virtualized mode, 43
OpenFlow overview, 7
OpenFlow pipeline
MAC group table, 33
Operational status, 102
OSPFv2, 14
OSPFv3, 14
OVS-OFCTL, 11

P

Passive mode, 18
Per-flow rate-limiters
Creating limiters, 42
flow, 42
Limiter details, 42
Per-flow rate-limiting
QoS vendor extensions, 42
PIM-DM, 14
PIM-SM, 14
Ping, 13
Pipeline modification process
table modification, 69
Policy engine
errors, 91
Policy engine table
restrictions, 88
Policy table metadata
L3 match
L3 miss, 34
Policy tables
rules, 34
Port ACLs, 13
Port modification commands, 12
Port security, 13
Programming flow errors
Error message programming flow, 87
Push/Pop VLAN
v3 Push/Pop VLAN, 63
PVST
interoperability, 14

Q

Q-in-Q, 13, 79
QoS vendor extensions
Per-flow rate-limiters, 42

R

Rate limiting, 13, 30
Rate-limiter, 42
Remote Mirror Endpoint, 79
Remote mirror endpoint, 13
RIP, 14
Router ACLs, 13
RSTP, 14

S

Service insertion
Overview, 108
service tunnels, 108

tunnels, 108
sFlow, 14
Show
OpenFlow, 49
Single-tagged packets
modification
addition, 90
SNTP, 13
Software flows, 18
Software rate limiting, 30
Source-IP, 52
Source-mac, 52
Source-port, 52
Static Multicast Routes, 14
Static Routes, 14
Statistics refresh rate, 74
STP, 14
STP loop guard, 14

T

Tagged/Untagged packets, 102
TCP/UDP
flags, 89
matching, 89
port ranges, 89
Technical support, 94
Telnet client and server, 13
TFTP, 13
TimeP, 13
Traceroute, 13
Transparent Mode, 79
Transparent mode, 13
TRmode, 13, 79
Tunneling, 11

U

UDLD, 14
UDP broadcast forwarder, 13
Unsupported features, 12

V

Verify routing, 31
Virtualization mode, 8, 103
Virus Throttling, 14
VLAN, 8, 9
ACLs, 13
errors, 82
VLAN-ID, 52
VLAN-priority, 52
VRRP, 14

W

Web auth, 13
Websites, 94
product manuals, 93