Multi-Service IronWare

Software Defined Networking (SDN) Configuration Guide

BROCADE

Supporting Multi-Service IronWare R05.6.00

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Multi-Service IronWare Software Defined Networking Configuration Guide	*53-1003034-01*	R05.6.00 document updated with enhancements in R05.5.00release	30 September, 2013

Contents

About This Document

In this chapter

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade device, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, MPLS, and VRRP.

Supported hardware and software

The following hardware platforms are supported by this release of this guide:

TABLE 1   Supported devices

Brocade NetIron XMR Series	Brocade MLX Series	NetIron CES 2000 and NetIron CER 2000 Series
Brocade NetIron XMR 4000	Brocade MLX-4	Brocade NetIron CES 2024C
Brocade NetIron XMR 8000	Brocade MLX-8	Brocade NetIron CES 2024F
Brocade NetIron XMR 16000	Brocade MLX-16	Brocade NetIron CES 2048C
Brocade NetIron XMR 32000	Brocade MLX-32	Brocade NetIron CES 2048CX
	Brocade MLXe-4	Brocade NetIron CES 2048F
	Brocade MLXe-8	Brocade NetIron CES 2048FX
	Brocade MLXe-16	Brocade NetIron CER 2024C
	Brocade MLXe-32	Brocade NetIron CER-RT 2024C
		Brocade NetIron CER 2024F
		Brocade NetIron CER-RT 2024F
		Brocade NetIron CER 2048C
		Brocade NetIron CER-RT 2048C
		Brocade NetIron CER 2048CX
		Brocade NetIron CER-RT 2048CX
		Brocade NetIron CER 2048F
		Brocade NetIron CER-RT 2048F
		Brocade NetIron CER 2048FX
		Brocade NetIron CER-RT 2048FX

Supported software

For the complete list of supported features and the summary of enhancements and configuration notes for this release, refer to the *Multi-Service IronWare R05.6.00 Release Notes*.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Notes, cautions, and danger notices

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Internet Explorer
Mozilla Corporation	Mozilla Firefox
Sun Microsystems	Java Runtime Environment

Related publications

For the latest edition of these documents, which contain the most up-to-date information, see Documentation at *http://www.brocade.com/ethernetproducts*

- *Multi-Service IronWare Administration Guide*
- *Multi-Service IronWare Security Configuration Guide*
- *Multi-Service IronWare Switching Configuration Guide*
- *Multi-Service IronWare Routing Configuration Guide*
- *Multi-Service IronWare Traffic Management Configuration Guide*
- *Multi-Service IronWare Multicast Configuration Guide*
- *Multi-Service IronWare Multiprotocol Label Switch (MPLS) Configuration Guide*
- *Multi-Service IronWare Software Defined Networking (SDN) Guide*
- *Brocade MLX Series and NetIron Family YANG Guide*
- *Brocade MLX Series and NetIron XMR Series Diagnostic Reference*
- *Unified IP MIB Reference*
- *Multi-Service IronWare Software Upgrade Procedures for Brocade MLX Series and NetIron Family devices*
- *Brocade MLXe Series Installation Guide*
- *Brocade MLX Series and Brocade NetIron XMR Installation Guide*
- *Brocade NetIron CES 2000 Series and Brocade NetIron CER 2000 Series Hardware Installation Guide*

Getting technical help or reporting errors

To contact Technical Support, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

In this chapter

OpenFlow

Table 2 lists the individual Brocade NetIron devices and the OpenFlow features they support.

TABLE 2   Supported Brocade OpenFlow features

Features supported	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
OpenFlow v1.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenFlow enabled on per-port basis (Hybrid switch mode)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenFlow Layer 3 Hybrid Port Mode	Yes	Yes	No	No	No	No	No
Maximum number of flows supported per-port	4096	4096	4096	4096	4096	4096	4096
OpenFlow scaling	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum number of flows supported per-system	128K	64K	4K	4K	4K	32K	32K
Support for hybrid port mode with protected VLANS and unprotacted VLANs on VPLS endpoint ports	Yes	Yes	No	No	No	No	No
Layer 2 OpenFlow match rules	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 3 OpenFlow match rules	Yes	Yes	No	No	No	No	No

TABLE 2   Supported Brocade OpenFlow features

Features supported	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
Simulteneous Layer2 and Layer3 support for OpenFlow	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Match both source and destination MAC addresses	Yes	Yes	No	No	No	No	No
Support for passive mode on the device	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenFlow actions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum flow statistics	4096	4096	2048	2048	2048	2048	2048
CLI command to delete a single flow or all flows in the flow table	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Overview of OpenFlow

An OpenFlow-enabled router supports an OpenFlow Client (control plane software), which communicates with an OpenFlow Controller using the OpenFlow protocol. The OpenFlow Controller runs on a server or a server cluster. OpenFlow-enabled routers support the abstraction of a flow table, which is manipulated by the OpenFlow Controller. The flow table contains flow entries. Each flow entry represents a flow (e.g. packets with a given MAC address, VLAN tag, IP address, or TCP/UDP port etc). The flow table is sorted by flow priority, which is defined by the controller. Highest priority flows are at the top of the flow table.

Incoming packets on an OpenFlow-enabled port are matched (in order of priority) against the flow entries defined for that port by the OpenFlow Controller. If the packet matches a given flow entry, the flow matching process stops, and the set of actions defined for that flow entry are performed. Packets that don't match any flow entry are dropped by default. The Brocade implementation supports an option to send such packets to the controller. Refer to *"Configuring the default action"*.

FIGURE 1   **OpenFlow-enabled router**
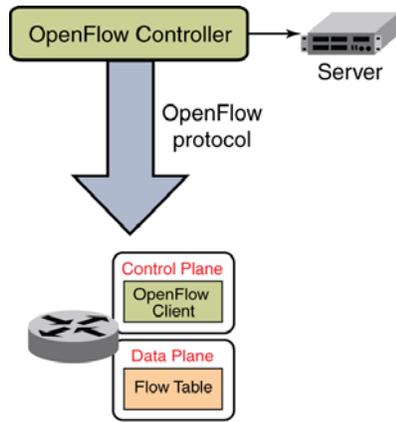
FIGURE 2   OpenFlow flow table entries
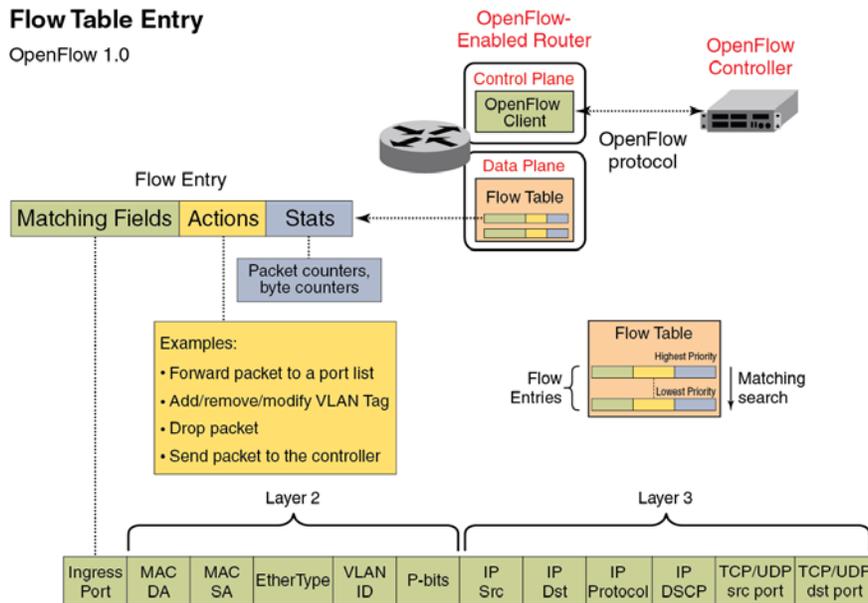
Flow table entries

Table 3 lists the OpenFlow match rules supported on Brocade devices. The implementation supports two modes of operation when enabling OpenFlow on a port: Layer 2 mode and Layer 3 mode. Layer 2 mode supports OpenFlow matching rules based on the Layer 2 fields shown in Figure 2, while Layer 3 mode supports the OpenFlow matching rules based on the Layer 3 fields.

The Brocade MLX Series and Brocade NetIron XMR devices support enabling ports in either Layer 2 or Layer 3 mode. The Brocade NetIron CER and Brocade NetIron CES devices support Layer 2 mode by default (OpenFlow Layer 3 mode configuration on a port is currently not supported on these devices).

TABLE 3   OpenFlow match rules

Match rule	Brocade MLX Series Brocade NetIron XMR	Brocade NetIron CER Brocade NetIron CES
Port enabled for Layer 2 mode	Yes	Yes
Source port	Yes	Yes
Source or destination MAC address	Yes These devices support either source or destination MAC address, or a combination of both source and destination MAC addresses as the match rule.	These devices support either source MAC or destination MAC address as the match rule, not both at the same time. This is a global option to be configured by the user.
Ether type	Yes	Yes
VLAN ID	Yes	Yes
VLAN priority	Yes	Yes
Untagged packets	Yes	Yes
Port enabled for Layer 3 mode	Yes	No
Ether type (Supports matching to Ether type value 0x88CC LLDP only; supports only 'send to controller' as the action)	Yes	No
Ether type (Supports matching to Ether type ARP value; supports only 'send to controller' as the action)	Yes	No
Source port	Yes	No
VLAN ID	Yes	No
VLAN priority	Yes	No
Source IP address	Yes	No
Destination IP address	Yes	No
Protocol type	Yes	No
IP TOS bits	Yes	No
TCP or UDP source port	Yes	No
TCP or UDP destination port	Yes	No

OpenFlow actions

Each OpenFlow flow table entry contains the list of actions to be performed when a packet matches the flow entry. These actions are defined by the OpenFlow Controller.

Packets that do not match any flow entry are dropped by default. The Brocade implementation supports an option to send such packets to the controller. Refer to "Configuring the default action".

Brocade devices support the actions listed in Table 4.

TABLE 4   OpenFlow actions supported on Brocade devices

OpenFlow action	Brocade MLX Series Brocade NetIron XMR	Brocade NetIron CER Brocade NetIron CES
Forward a packet to a set of ports	Yes	Yes
Drop the packet	Yes	Yes
Add, modify, or remove VLAN ID or priority on a per destination port basis	Yes	Yes
Modify the IP DSCP (for a flow sending a copy of the packet to multiple destinations, the DSCP modification must be the same for all destinations. Modifying IP DSCP is only supported on ports enabled with Layer 3 mode.)	Yes	No
Modify the source or destination MAC address (for a flow sending a copy of the packet to multiple destinations, the MAC address modification must be the same for all destinations).	Yes	No
Send the packet to the controller (Packet In)	Yes	Yes
Receive the packet from the controller and send it to ports (Packet Out)	Yes	Yes

OpenFlow Controller

Multiple controller connections can be used for redundancy purposes, such as when using a single controller with multiple addresses. Multiple controller connections can also be used to support active-standby controllers.

Regardless of the intended use of multiple controller connections, the Brocade device allows all the controller connections to concurrently manage the flow table. That is, flow entries in the flow table are not identified as belonging to any specific controller connection. In an active-standby controller deployment, controllers themselves must coordinate their actions and active-standby states. The Brocade device will respond to all connected controllers without distinction.

The Brocade device supports two types of controller connections (also called modes): active and passive. An active connection is one for which the Brocade device will initiate (seek) the TCP connection to a given OpenFlow Controller address. With a passive connection, the Brocade device will passively wait for the controller to initiate (seek) the TCP connection to the Brocade device. Active mode is commonly used with production controllers, while passive mode is commonly used for testing purposes in experimental environments. Optionally, a controller connection can also use SSL encryption.

OpenFlow counters

Brocade MLX Series and Brocade NetIron XMR devices record the number of received packets and bytes on a per-flow basis. However, recording the number of received bytes on a per-flow basis is only supported on ports on the 8x10G or 100G cards. Brocade NetIron CER and Brocade NetIron CES devices record only the received packets on a per-flow basis—these devices do not record the number of bytes per flow.

The following per port counters are available in the flow table:

TABLE 5   OpenFlow counters supported on devices

Counter	Description	Brocade MLX Series Brocade NetIron XMR	Brocade NetIron CER Brocade NetIron CES
Received packets	Number of packets received on the port	Yes	Yes
Transmitted packets	Number of packets transmitted from the port	Yes	Yes
Received bytes	Number of bytes received on the port	Yes	No
Transmitted bytes	Number of bytes transmitted from the port	Yes	Yes
Receive drops	Number of received packets dropped on the port because the packets did not match any rules	Yes	Yes
Transmit drops	Number of transmit packets dropped on the egress port	Yes	Yes
Receive errors	Number of errors detected on the port on received packets	Yes	Yes
Transmit errors	Number of errors detected on the port on transmitted packets	Yes	Yes
Receive frame alignment errors	Number of frame alignment errors detected on packets received on the port	Yes	No
Receive overrun errors	Number of packets that caused overrun in the receive buffer on the port	Yes	No
Receive CRC errors	Number of packets received on the port that had CRC errors	Yes	No
Collisions	Number of collisions recorded on the port	Yes	No

The following table lists the per-flow counters available:

TABLE 6   Per-flow OpenFlow counters supported

Counter	Description	Brocade MLX Series Brocade NetIron XMR	Brocade NetIron CER Brocade NetIron CES
Received packets	Number of packets received per flow	Yes	Yes
Received bytes	Number of bytes received per flow	Only on 8x10G or 100G cards	No

Considerations and limitations

Brocade devices support version 1.0.0 of the OpenFlow protocol. Consider the following points when you configure OpenFlow on devices.

- OpenFlow must be enabled globally on the device before you can enable interfaces for OpenFlow.
- You must explicitly enable or disable OpenFlow on each interface using the CLI commands. You cannot use a range of ports to enable OpenFlow on them.

- Before you can disable OpenFlow globally on the device, you must disable OpenFlow on all interfaces individually.

- Spanning tree protocol and other Layer 2 or Layer 3 protocols are not supported on OpenFlow-enabled ports.

- Support up to three concurrent sessions with a maximum of two concurrent SSL sessions.

- Up to 3000 configured flows are supported if all the flows are with a wildcard for the incoming port.

- Local and normal actions defined by the OpenFlow 1.0 protocol are not supported.

- After a reboot, a delay of 16 seconds for Brocade NetIron CER and Brocade NetIron CES devices, and 180 seconds for Brocade MLX Series and Brocade NetIron XMR devices is added before any flows can be pushed. This is the default delay time to allow all modules and ports to come up.

- 8x10GbE and 2x100GbE interface modules support all generic Ethertype value in L2 mode. All other interface modules support Ethertype 0x88CC (LLDP) only in L2 mode.

- On OpenFlow-enabled ports, packets that do not match any flow entry are dropped by default. Although the OpenFlow 1.0 protocol specifies sending such packets to the controller as mandatory, the Brocade implementation adopted the latest behavior defined in the OpenFlow 1.2 protocol, which specifies that such packets MAY be sent to the controller or MAY be dropped by router configuration. The Brocade implementation supports an option to send such packets to the controller. Refer to "Configuring the default action".

In addition, the following restrictions apply:

Brocade NetIron CER and Brocade NetIron CES devices

- Enabling ports for Layer 3 flows is not supported.

- Either Source MAC address or Destination MAC address can be used as a matching rule. The choice is a device-level configuration that you specify at the time of enabling OpenFlow on the device.

- Statistics are available only for up to 2048 flows on a first-come-first-served basis.

Brocade MLX Series and Brocade NetIron XMR devices

- Even though modification of the source and destination MAC address fields of a packet is supported, modification on a per-destination port basis for multi-destination flows is not supported.

  In other words, sending a packet to multiple ports and having the MAC addresses modified on a per-destination port basis is not supported. However, sending a packet to multiple ports and having the MAC addresses modified in the same way for all destination ports is supported. Similar restriction applies to modifications of the DSCP field of packets.

- Modification of VLAN tag (such as adding, removing, modifying, or modifying the PCP bits of a tag) is supported on a per-destination port basis for tagged packets. A flow may specify sending a copy of a packet to multiple destination ports and have each copy of the packet tagged with a different VLAN ID.

  At the same time, if the rule is to send a tagged packet to multiple outgoing ports with different VLAN tags, and if the action for one of the outgoing ports is to send the packet as untagged, the packet is still tagged with the VLAN ID of 0 on that port. For egress ports with the action specifying modified VLAN tag, the specified VLAN tag itself is added.

- An action to modify the VLAN priority of an untagged frame will result in a VLAN tag being added to the frame. If the action does not specify a VLAN ID value, the VLAN ID will be set to 0.
- The action to modify IP DSCP is only supported for flows on ports enabled for Layer 3 mode.
- Matching a VLAN ID on a Layer 3 mode port is only supported for packets with an IP payload.

Hybrid switch and OpenFlow hybrid port mode

Hybrid Switch Mode

The Brocade device supports enabling OpenFlow on a per-port basis, so you can choose which ports of the device will be controlled by the OpenFlow feature. Non-OpenFlow-enabled ports continue to support existing features of the device such as MPLS, VPLS, IPv4 or IPv6 routing Layer 2 switching.

Hybrid Port Mode

OpenFlow hybrid-enabled ports support both OpenFlow traffic forwarding and normal routing traffic forwarding. OpenFlow hybrid-enabled ports support "protected VLANs" and "unprotected VLANs". Protected VLANs are not subject to defined OpenFlow flows on the OpenFlow hybrid-enabled ports. OpenFlow flows on a hybrid-enabled port will not match any traffic on protected VLANs. Unprotected VLANs are subject to defined OpenFlow flows on the OpenFlow hybrid-enabled port. OpenFlow flows on a hybrid-enabled port are allowed to match on the traffic of unprotected VLANs.

Figure 3 shows a topology in which port 1/1 on Device-1 and port 1/4 on Device-2 are hybrid-enabled OpenFlow ports with VLAN 10 as a configured protected VLAN. By configuring a virtual ethernet on a protected VLAN 10 and assigning an address to route the traffic of the nodes, you are able to send protected VLAN traffic between the nodes and route the traffic as per the virtual interface. Traffic flowing on other VEs created on top of other VLANs (the unprotected VLANs) treated as unprotected VLAN traffic and is subject to OpenFlow rules lookup. OpenFlow traffic can be forwarded through this port.

FIGURE 3   **OpenFlow hybrid port mode topology**
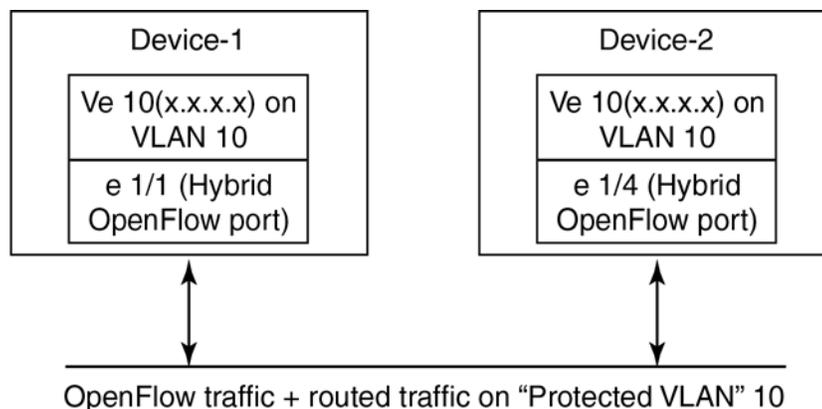
Hybrid port mode operation

Consider Device-1 in Figure 3. Ingress traffic on VLAN 10 on hybrid port 1/1 will be processed for IPv4 and IPv6 unicast routing. Traffic on other VLANs will be processed against OpenFlow flows on port 1/1 and switched accordingly. A preconfigured number of protected VLANs can be supported for normal routing. The Spanning tree protocols (STP) state of these routing VLANs will be set to forwarding, as the Layer 2 protocol is not supported.

Configuring OpenFlow hybrid port mode

1. Enable OpenFlow at the global configuration level.

2. Configure OpenFlow controller configurations.

3. Configure the system maximum configuration for the maximum OpenFlow entries. (The default is 0.)

4. Configure the maximum OpenFlow flow-protected VLAN entries. (The default is 0.)

NOTE
System reload is required once you change the system maximum values.

5. Configure the maximum OpenFlow unprotected VLAN entries. (The default is 0.)

6. Configure protected VLANs on the port. A maximum of 40 protected VLANs can be configured on an OpenFlow port.

7. Enable OpenFlow hybrid port mode on the desired interfaces.

8. Configure a VE for the interface by specifying the protected VLAN and add routing entries.

Feature information

- Switchover and HLOS are not supported. When the active management processor (MP) goes down, communication with the controller is brought down and the flow tables on the MP and all line processors (LP) are cleared. The connection with the controller is re-established after switchover.

- When LP is reset, the flow table on the LP is restored once the LP comes up and flows specific to that LP are maintained in the MP.

- When an OpenFlow-enabled port goes up or down, no rules are removed. The addition or deletion of rules depends solely on the controller.

- 4K OpenFlow entries are supported.

- Up to 2K protected VLANs per system are supported.

Capabilitiess and prerequisites

Brocade devices support version 1.0.0 of the OpenFlow protocol. The following are current capabilities and prerequisites of OpenFlow hybrid port mode.

- IPV4 and IPv6 unicast routing are supported on OpenFlow protected and unprotected VLANs.

- Packets tagged with a protected VLAN id:

- Packets tagged with a protected VLAN id will be forwarded by IPv4 and IPv6 unicast routing, if IPv4 or IPv6 routing is configured on that VLAN. If IPv4 or IPv6 routing is not configured on that VLAN, such packets will be dropped.

- Packets tagged with an unprotected VLAN id:

  - Packets tagged with an unprotected VLAN id will be subject first to OpenFlow flows. If there is a match on an OpenFlow flow, the packet will be forwarded according to the flow actions. No further IPv4 or IPv6 routing is supported for packets that are forwarded by OpenFlow flows. If there is no match on any OpenFlow flow, the packet will be forwarded by IPv4 or IPv6 unicast routing, if IPv4 or IPv6 routing is configured on the VLAN. If IPv4 or IPv6 routing is not configured on the VLAN, those packets are either dropped or sent to the controller, per OpenFlow configuration..

- Layer 2 or L2VPN forwarding is not supported on ports in hybrid-enabled ports because MAC learning is disabled on these ports.

- A port can be enabled for hybrid port mode only if the port is untagged in the default VLAN.

- Ports in OpenFlow hybrid port mode cannot be added as untagged ports to regular VLANs or L2VPN because this can cause a problem with topology discovery.

- As routing is enabled on a port in hybrid port mode, OpenFlow traffic or unprotected VLAN traffic sent with destination MAC address as the port's MAC address and matching IP route entries on the port can potentially find its VLAN and MAC address modified unless the OpenFlow rules explicitly set the VLAN and destination MAC address in the outgoing packet.

- Inbound normal ACL configuration is not supported on the port in hybrid port mode.

- Any port with the default VLAN not equal to the system default VLAN ID cannot be enabled for hybrid port mode.

- Policy based routing (PBR) is not supported.

- Protected VLAN traffic that does not have matching IP route entries will be dropped.

- Multiple interfaces cannot be part of a VE created on a port in hybrid port mode with a protected VLAN.

- BGP, OSPF and IS-IS protocols are supported on protected VLANs:

  NOTE
  Layer2 or L2VPN, VRF are not supported.

- When protected VLANs are configured but the port is not part of the VLAN, the traffic coming on the port with the protected VLAN will be dropped.

- Port in hybrid-enabled OpenFlow doesn't support MPLS running on the same port.

- Link aggregation is not supported.

Enabling OpenFlow hybrid port mode

Use **openflow enable** command to enable or disable hybrid port mode on the port and the port becomes a normal port on an interface. The **no** version of the command disables the hybrid port mode on the port and the port becomes a normal port.

```
Brocade(config-if-e10000-2/5)# openflow enable layer2 hybrid-mode
```

Syntax: **[no] openflow enable layer2 | layer3** [hybrid-mode]

Adding or Deleting protected VLANs

Use **openflow protected -vlans** to add or delete protected VLANs on a hybrid port-mode interface. The **no** form of the command deletes the configured protected VLANs from the hybrid-enabled port.

```
Brocade(config-if-e10000-2/5)# openflow protected-vlans 10
```

Syntax: **[no] openflow protected-vlans** *id1 id2 ...idn*

VLANs can be configured individually.

NOTE
A VLAN range is not specified for this command .

Setting the system maximum

The **system-max openflow-pvlan-entries** command sets the CAM size of OpenFlow protected VLAN entries for the device. By default, this value is set to 0.

```
Brocade(config)# system-max openflow-pvlan-entries 2000
```

Syntax: **system-max openflow-pvlan-entries** *value*

The **value** variable represents the number of port and protected VLAN combination entries that can be configured in the system. The range is from 0 to 2048. after using this command, you must reload the system.

The **system-max openflow-unprotectedvlan-entries** command sets the CAM size of OpenFlow unprotected VLAN entries for the device. By default, this value is set to 0.

```
Brocade(config)# system-max openflow-unprotectedvlan-entries 1000
```

Syntax: **system-max openflow-unprotectedvlan-entries** *value*

The **value** variable represents the number of port and unprotected VLAN combination entries that can be configured in the system. The range is from 0 to 2048. after using this command, you must reload the system.

Displaying OpenFlow configuration information

The show OpenFlow command displays the configuration for OpenFlow.

```
Brocade(config)# show openflow
Number of Controllers:        2

Controller 1:
Connection Mode:        passive, TCP,
Listening Address:      0.0.0.0
Connection Port:        6633
Connection Status:
SSL Connection         :False
No TCP connection found.

Controller 2:
Connection Mode:        active, TCP,
Controller Address:      10.20.101.199
Connection Port:        23
Connection Status:
```

```
Local IP address:port <-> Remote IP address:port TCP state    RcvQue  RxBuffe
SendQue TxBuffe
10.20.178.73   8807    10.20.101.199  23    ESTABLISHED 0     0      0
0
SSL Connection       :False
Match Capabilty:
L2: Port, Source MAC, Destination MAC, Ether type, Vlan, Vlan PCP
L3: Port, Vlan, Vlan PCP, Source IP, Destination IP, IP Protocol, IP TOS, IP Src
Port, IP Dst Port

Normal Openflow Enabled Ports:     e2/1
Hybrid Mode ports        Protected Vlan-IDs
e4/1                     (100,101,102,103)
e7/2                     (200)
Default action: drop
Maximum number of flows allowed: 4096
Maximum number of Protected Vlans allowed: 2048
```

Rate limiting capabilities on OpenFlow enabled ports

Rate-limiting support on OpenFlow enabled ports:

- OpenFlow ports (non-hybrid port mode ports): Normal CLI configuration of port-based rate limiting is supported. Per VLAN rate limiting not supported.
- Hybrid port mode ports: Normal CLI configuration of port-based rate limiting is supported. VLAN-based rate limiting supported on protected and unprotected configured VLANs.
- You must set the rate control for certain protocols at the global configuration level.

NOTE
Rate control for certain protocols, such as ARP, will be based on the global configuration. For a very large burst of ARP traffic on a port, which may not be a normal scenario but could happen, the system could become unresponsive.

VPLS support for VLANs on OpenFlow hybrid mode ports

This feature supports VPLS switching or routing for protected VLANS and for configured unprotected VLANS on OpenFlow hybrid mode ports. It is supported on Layer2, Layer3 and Layer23 OpenFlow hybrid mode ports.

Limitations

- VPLS VLANs cannot be configured as Untagged VLANs on OpenFlow hybrid mode ports.
- System-max OpenFlow unprotected VLANs are limited to 4K. This number is utilized by both L2 VLANs as well as VPLS VLANs.
- L2 Switching is not supported on OpenFlow hybrid mode ports.
- Dual tagged VPLS Instances are not supported on OpenFlow hybrid mode ports.
- IGMP snooping is not supported on configured unprotected VLANs.

FIGURE 4   Packet flow diagram
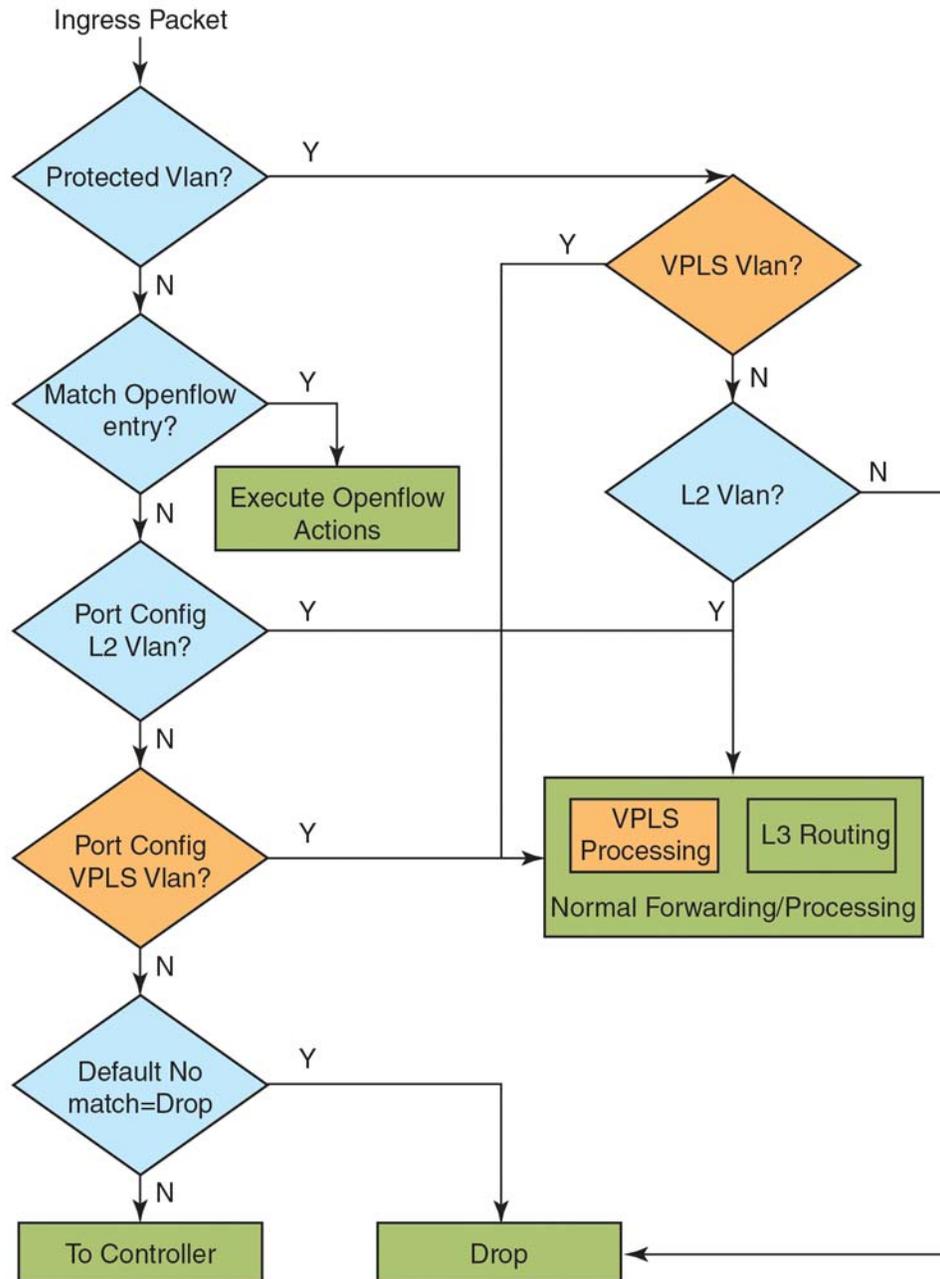
Sample configurations

VPLS support to configure OpenFlow hybrid mode port

For VPLS instance, you can configure a port as an OpenFlow hybrid mode port by executing these commands.

```
Brocade(config)#
Brocade(config)#router mpls
```

```
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow enable layer2 hybrid-mode
```

Check for global system-max unprotected VLAN number, while configuring a port as a hybrid port. If the system-max unprotected VLAN number exceeds the maximum permissible, the port is rejected from being configured as a hybrid mode port. Otherwise VPLS VLAN becomes the configured unprotected VLAN on the port.

VPLS support on configured protected VLANs

These are the steps taken to configure VLAN as an OpenFlow protected VLAN.

- Enable OpenFlow globally and configure system-max for OpenFlow entries.
- Configure OpenFlow controller.
- Configure system-max for Protected VLAN entries.
- Enable OpenFlow hybrid on port.
- Configure Protected VLAN for port.
- Configure VPLS instance on the port using the same configured Protected VLAN.

To configure VLAN as an OpenFlow protected VLAN, execute the following commands.

```
Brocade(config)#
Brocade(config)#router mpls
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow protected-vlans 100
```

NOTE
Check for port based maximum protected VLAN number (which is 40). If exceeded, you will get an error message , and the VLAN will not be configured as a protected VLAN.

NOTE
If system-max protected VLANs exceeds 2K, then you will get an error message , and the system will not configure the VLAN as protected VLAN.

VPLS instance to enable OpenFlow hybrid mode port on protected VLAN

Once protected VLANs have been configured, to enable OpenFlow hybrid mode port, use the following commands to create a VPLS instance.

```
Brocade(config)#
Brocade(config)#router mpls
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
```

```
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow protected-vlans 100
Brocade(config-if-e10000-2/8)#openflow enable layer2 hybrid-mode
```

Since this protected VLAN has become part of VPLS VLAN on this port, VPLS switching on this protected VLAN will be supported.

Deleting VPLS instances from protected VLAN

To remove VPLS instance for protected VLAN from OpenFlow hybrid mode port, use this sequence of commands.

```
Brocade(config)#
Brocade(config)#router mpls
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow protected-vlans 100
Brocade(config-if-e10000-2/8)#openflow enable layer2 hybrid-mode
Brocade(config)#
Brocade(config)#
Brocade(config)#router mpls
Brocade(config)#vpls v1 100
Brocade(config)#vlan 100
Brocade(config)#no tag e 2/8
```
Now this port is not a part of VPLS instance. The protected vlan will become unconfigured protected vlan. It will drop.

NOTE

When removing protected VLAN configuration, do not exceed the system-max unprotected VLAN number. The command will be rejected and you will get an error message.

After removing the protected VLAN configuration, this VPLS VLAN will become configured as an unprotected VLAN. Now, It will do VPLS switching in absence of matching flow.

Deleting VPLS instances from unprotected VLAN

To remove OpenFlow hybrid mode from a port with unconfigured protected VLAN and a VPLS instance, execute the following commands.

```
Brocade(config)#
Brocade(config)#router mpls
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow protected-vlans 100
Brocade(config-if-e10000-2/8)#openflow enable layer2 hybrid-mode
Brocade(config)#
Brocade(config)#router mpls
Brocade(config)#vpls v1 100
Brocade(config)#vlan 100
```

```
Brocade(config)#no tag e 2/8
```

Now that, the port has become a normal port and VPLS instance is configured on the port, It will do VPLS processing for that VLAN.

To remove OpenFlow hybrid mode from a port with configured unprotected VLAN and a VPLS instance, execute the following commands.

```
Brocade(config)#
Brocade(config)#router mpls
Brocade(config-mpls)#
Brocade(config-mpls)#vpls v1 100
Brocade(config-mpls)#vpls-peer 17.17.17.17
Brocade(config-mpls-vpls-v1)#vlan 100
Brocade(config-mpls-vpls-v8-vlan-100)#tag e 2/8
Brocade(config-mpls)#int e 2/8
Brocade(config-if-e10000-2/8)#openflow enable layer2 hybrid-mode
Brocade(config)#
Brocade(config-if-e10000-2/8)#no openflow enable layer2 hybrid-mode
```

Configuring OpenFlow

With this feature, you can enable OpenFlow on an interface with Layer23 option in order to support Layer 2 and Layer 3 flows on that interface. Layer23 option supports the hybrid mode OpenFlow also. Configured with the Layer23 option, controller can configure flows with L2 and L3 parameters together. A flow can contain these fields, Ingress port, MAC DA, MAC SA, Ethertype, VLAN ID , P-bits, IP Src, IP Dst, IP protocol and IP DSCP.

By default, the OpenFlow feature is disabled on Brocade devices. You must first enable the OpenFlow feature on the device before you can configure the parameters on the device.

Enabling OpenFlow on devices

After you enable OpenFlow on the device, you can enable OpenFlow on specific interfaces and configure additional OpenFlow parameters on them.

Enabling OpenFlow on Brocade MLX Series and Brocade NetIron XMR devices

Enter the following command:

```
Brocade(config)# openflow enable ofv100
```

Syntax: [no] openflow enable ofv100

The **ofv100** keyword specifies the OpenFlow protocol version supported. Currently, Brocade devices support OpenFlow protocol version 1.0.0.

Use the **[no]** version of the command to disable OpenFlow feature on the device.

NOTE
You must disable OpenFlow on all interfaces individually before you can disable OpenFlow globally on the device.

Enabling OpenFlow on Brocade NetIron CER and Brocade NetIron CES devices

You can optionally specify the MAC address match rule capability as either source MAC or destination MAC address. Default is destination MAC address. On these devices, you cannot change the MAC address match option dynamically. You must first disable the current mode and then enable the new option. Changing the MAC address match option will clear all existing OpenFlow configuration and OpenFlow flow table content.

Enter the following command:

```
Brocade(config)# openflow enable ofv100
```

Syntax: [no] openflow enable ofv100 *src-mac*

The **src-mac** keyword specifies the source MAC address matching option.

Use the **[no]** version of the command to disable OpenFlow feature on the device.

NOTE
You must disable OpenFlow on all interfaces individually before you can disable OpenFlow globally on the device.

Enabling OpenFlow on a specified interface

After you have enabled the OpenFlow feature on the device, you can enable OpenFlow on specific interfaces.

NOTE
You can enable OpenFlow on an interface only after you have enabled OpenFlow globally on the device. In addition, you must use individual CLI commands to enable OpenFlow on each interface. You cannot specify a range of ports when enabling OpenFlow on them.

On Brocade NetIron CER and Brocade NetIron CES devices:
Enter the following command:

```
Brocade(config-if-e1000-1/1)# openflow enable
```

Syntax: [no] openflow enable *layer2 | layer23 [hybrid-mode]*

Use the **[no]** version of the command to disable OpenFlow on the interface. By default, the port is enabled for Layer 2 matching mode, since Brocade NetIron CER and Brocade NetIron CES devices currently do not support Layer 3 matching mode. Layer23 can be enabled with hybrid mode. If hybrid mode is enabled, that interface will support protected and unprotected VLANs similar to Layer 2 hybrid and Layer 3 hybrid.

On Brocade MLX Series and Brocade NetIron XMR devices:
Enter the following command:

```
Brocade(config-if-e1000-1/1)# openflow enable layer2
Or
```

```
Brocade(config-if-e1000-1/1)# openflow enable layer3
Brocade(config-if-e1000-1/1)# openflow enable layer23
```

Syntax: [no] openflow enable *layer2 | layer3 | layer23 [hybrid-mode]*

You can specify Layer 2 or Layer 3 or both layers in hybrid mode as Layer23 matching mode to be supported on the interface. By default, interfaces on these devices support Layer 2 matching mode. If you enable Layer 2 matching mode on the specified interface, only Layer 2 matching fields are supported on that interface.

Flow validation

These validations are required before programming flows on Layer23 port.

- When IP fields exist in rule then ether_type must be 0x800.
- IPv6 rules are not supported on Layer23 port. (But IPv6 ether_type without IPv6 parameters is supported.)

Flow action

OpenFlow actions are not changed for Layer23 support. All actions currently supporting to Layer 2 or Layer 3 flows will continue to be supported. Actions currently supported are listed separately for Brocade MLX Series and Brocade NetIron XMR devices, Brocade NetIron CER and Brocade NetIron CES devices.

On Brocade MLX Series and Brocade NetIron XMR devices:

When a matching flow entry is found, a set of actions can be applied for processing the packet. The system supports the following actions:

- Forward to a port.
- Forward to a set of ports.
- Forward to a controller.
- Forward a packet received from a controller to a port or set of ports.
- Drop the packet.
- Keep, add, modify or remove VLAN ID, VLAN priority. Modify VLAN ID per port is also supported, i.e., each destination port can send a packet with a different VLAN ID for the same matching rule.
- Modify source MAC address and destination MAC address for both Layer 2 and Layer 3 IPv4 flows.

On Brocade NetIron CER and Brocade NetIron CES devices:

When a matching flow entry is found, a set of actions can be applied for processing the packet. The system supports the following actions:

- Forward to a port.
- Forward to a set of ports.
- Forward to a controller.
- Forward a packet received from a controller to a port or set of ports.
- Drop the packet.
- Keep, add, modify or remove VLAN ID, VLAN priority. Modify VLAN ID per port is also supported, i.e., each destination port can send a packet with a different VLAN ID for the same matching rule.

Setting the system maximum

The **system-max openflow-pvlan-entries** command sets the CAM size of OpenFlow protected VLAN entries for the device. By default, this value is set to 0.

```
Brocade(config)# system-max openflow-pvlan-entries 2000
```

Syntax: **system-max openflow-pvlan-entries** *value*

The **value** variable represents the number of port and protected VLAN combination entries that can be configured in the system. The range is from 0 to 2048. after using this command, you must reload the system.

The **system-max openflow-unprotectedvlan-entries** command sets the CAM size of OpenFlow unprotected VLAN entries for the device. By default, this value is set to 0.

```
Brocade(config)# system-max openflow-unprotectedvlan-entries 1000
```

Syntax: **system-max openflow-unprotectedvlan-entries** *value*

The **value** variable represents the number of port and unprotected VLAN combination entries that can be configured in the system. The range is from 0 to 2048. after using this command, you must reload the system.

For Brocade Multiservice Ironware Guide release 5.6, a new command has been added forlayer2or3 and layer23 flows.

Syntax: **system-max np-openflow-entries** layer2or3 | layer23IPv4 *value* slot [*i j k* | *i to z* | *all*]

The following parameters are available for this command:

- layer2or3 -both layer 2 flow or layer 3 flow entries
- Layer23IPv4 - Layer23 including L2 and IPv4 flow entries

The above layer2or3 or layer23IPv4 options are optional (atleast one of them have to be specified).

- Slot number can be any of the valid slot number in the device. For slots, you can provide "all", "slot 1 to 2" and individual slot options.
- Slot number mentioned in a single command need not be of same card type.
- If any of the option layer2or3 or layer23IPv4 is not applicable for a particular card on a slot, it is ignored.
- You can have multiple lines of above command to have different sets of values for different set of modules.

NOTE

This command is only applicable for Brocade MLX Series and Brocade NetIron XMR devices.

Connecting to an OpenFlow controller

To connect to a controller in active mode, enter the following command:

```
Brocade(config)# openflow controller ip-address 10.2.3.4
```

Syntax: **[no] openflow controller ip-address** *ip-address* **[no-ssl] [port** *port]*

The **ip-address** keyword specifies the IP address of the Controller. By default, the connection with the Controller uses SSL encryption, but you can optionally disable SSL encryption using the **no-ssl** keyword. By default, the OpenFlow connection uses TCP port 6633, but you can specify another port using the **port** keyword.

Use the **[no]** version of the command to remove the specified OpenFlow Controller connection.

To connect to a controller in the passive mode, enter the following command:

```
Brocade(config)# openflow controller passive no-ssl
```

Syntax: [no] openflow controller passive no-ssl [ip-address *ip-address*] [**port** *port*]

The **passive** keyword specifies that the device is in the passive mode. You can optionally specify the TCP port to be used for the connection. By default, the device accepts the connection from a controller with any IP address. However, you can provide an IP address to limit which controller can connect to the device.

Use the **[no]** version of the command to remove a passive connection. Passive mode connections are intended for testing environments and not recommended for production environments.

Setting up SSL encryption for controller connections

By default, a connection to the controller uses SSL encryption. To set up SSL connection, copy the SSL certificate and SSL client private key from the remote machine where you generated these into the device's flash using the following commands:

```
copy tftp flash <remote ip> <remote file> client-certificate
copy tftp flash <remote ip> <remote file> client-private-key
```

Syntax: copy tftp flash *remote ip*|*remote file* **client-certificate**

and

Syntax: copy tftp flash *remote ip*|*remote file* **client-private-key**

The **remote ip** parameter specifies the IP address of the remote machine from which the SSL client certificate is being copied.

The **remote file** parameter specifies the filename of the client certificate in the first command, and the client private key in the second command.

For each controller, you must enter both the commands. The device can store up to three SSL certificates and client private keys. If you remove a controller connection, you will need to delete the SSL certificates and client private keys from the device's flash memory using the monitor mode commands.

Disabling an SSL client

You can disable the SSL client within the device using the following command:

```
Brocade# ip ssl client disable
```

Syntax: [no] ip ssl client disable

After you disable an SSL client in the device, the corresponding controller connection that used SSL encryption will fail. However, you can reenable the controller connection by removing the SSL encryption option from the controller connection. Use the **[no-ssl]** option in the **openflow controller ip-address** *ip-address* **[no-ssl] [port** *port*] command to disable SSL encryption in the connection.

To reenable SSL client in the device, use the [no] version of the command.

Configuring multiple controller connections

Brocade devices support up to three controller connections. You can configure these connections with active or passive modes, in any combination, such as all active, all passive, or some active and some passive. Each connection requires its own separate command. To configure these, you enter separate commands. You can remove any of these connections using the [no] version of the command. The following example shows how you configure three connections.

```
Brocade(config)# openflow controller ip-address 10.2.3.4 no-ssl port 6635
Brocade(config)# openflow controller ip-address 10.2.3.5 no-ssl
Brocade(config)# openflow controller passive no-ssl ip-address 10.2.3.6
```

Configuring the system parameters for OpenFlow

You can specify the limit for OpenFlow flow table entries in the flow table. Enter the following command:

```
Brocade(config)# system-max openflow-flow-entries <limit>
```

Syntax: **system-max openflow-flow-entries** *limit*

The range is 0 to 4096. Specify the maximum number of flow table entries. This command requires a reboot to take effect. The default number of flow table entries is zero. To verify the flow table entry limit, use the **show openflow** command.

NOTE
This command is not available on the Brocade NetIron CER and Brocade NetIron CES devices. The default number of flows table entries is 4096 on these devices.

Configuring the default action

By default, the device drops packets that do not match any of the programmed flows. However, you can configure a device-level option to forward the packets to the controller instead of dropping them. This is an optional configuration. If this option is not configured, packets that do not match any flow entries on a port are dropped. When sending a packet to the controller, a copy of the packet is sent to each of the configured controller connections.

To enable this option, enter the following command:

```
Brocade(config)# openflow default send-to-controller
```

Syntax: **[no] openflow default send-to-controller**

Packets that match a flow entry on a port are processed according to the action specified and are not affected by this setting. Use the [no] version of the command to set the default action to drop such packets instead.

Displaying the OpenFlow status on the device

After enabling or disabling OpenFlow on a device, you can verify the configuration using any of the **show** commands.

Use the show running configuration command:

When OpenFlow is enabled on the device, the **show running configuration** command displays output similar to the following:

```
Brocade(config)# show run
Current configuration:
ver V5.4.0iT183
mirror ethernet 1/19
openflow enable ofv100
```

Show command

The show OpenFlow command displays the configuration for OpenFlow. It includes the configured unprotected VLANs as well.

```
Brocade(config)# show openflow

Administrative Status:        Enabled
SSL Status:                   Enabled

Controller Type:              OFV 100
Number of Controllers:        1

Controller 1:
Connection Mode:        passive, TCP,
Listening Address:      0.0.0.0
Connection Port:        6633
Connection Status:       TCP_LISTENING

Match Capability:
L2 : Port, Source MAC, Destination MAC, Ether type, Vlan, Vlan PCP
L3 : Port, Vlan, Vlan PCP, Ethertype(IP,ARP,LLDP), Source IP, Destination IP, IP
Protocol, IP TOS, IP Src Port, IP Dst Port
L23: All

Normal Openflow Enabled Ports:
Openflow Hybrid Interfaces:
e1/1
Protected VLANs   : None
Unprotected VLANs :    2, 3, 4, 5, 6, 7, 8, 9, 10, 11
....................................................
....................................................
3994, 3995, 3996, 3997, 3998, 3999, 4000, 4001, 4011,

e2/1
Protected VLANs   : None
Unprotected VLANs :  4010,

Default action: drop
Maximum number of flows allowed: 65536
Active flow: 0

Maximum number of Protected Vlans allowed: 2048
Maximum number of Unprotected Vlans allowed: 4096
Total number of Unprotected Vlans: 4002
```

Syntax: show openflow

Displaying the OpenFlow status

If OpenFlow is enabled on a device, you can get detailed report of the OpenFlow status on that device.

Brocade NetIron CER and Brocade NetIron CES devices:

On these devices, only Layer 2 matching mode is supported on the interfaces.

```
Brocade(config)# show openflow interface
Port  Link  Port-State Speed  Tag MAC            OF-portid  Name    Mode
1/1   Up    Forward    1G     No  0000.00b4.89c1  1                 Layer2
1/2   Up    Forward    1G     No  0000.00b4.89c2  2                 Layer2
1/3   Up    Forward    1G     No  0000.00b4.89c3  3                 Layer2
```

Brocade MLX Series and Brocade NetIron XMR devices:

```
Brocade(config)# show openflow interface
Port  Link Port-State  Speed Tag MAC            OF-portid  Name        Mode
1/5   Up   Forward     1G    No  0000.0088.0904    5       OpenFlow-A Layer2
1/7   Up   Forward     1G    No  0000.0088.0906    7       OpenFlow-B Layer3
1/8   Up   Forward     1G    No  0000.0088.0907    8       OpenFlow-C Layer3
2/1   Up   Forward     1G    Yes 0000.0088.0916    49      OpenFlow-E Layer2
```

TABLE 7 Output fields of the show openflow interface command

Field	Description
Port	Indicates the port number on the device.
Link	Indicates the link status.
Port-State	Indicates the action to be performed on packets that reach the interface. Supported actions include forward the packet, modify the VLAN tag, drop the packet, and send to the controllers.
Speed	Indicates the port speed.
Tag	Indicates whether the interface can accept tagged packets or not.
MAC	Indicates the MAC address of the port.
OF-PortID	Indicates the OpenFlow port ID that is assigned to the port on the device. Port numbers on the device are mapped to OpenFlow port IDs. For more information, see "Behavior of ports and devices".
Name	Indicates the name assigned to the port.
Mode	Indicates the OpenFlow mode enabled on the port. Ports on Brocade NetIron CER and Brocade NetIron CES devices support only Layer 2 mode. Ports on Brocade MLX Series and Brocade NetIron XMR devices support either Layer 2 or Layer 3 mode.

In addition, you can use the **show interface** command at the interface level. If OpenFlow is enabled on the interface, the OpenFlow status is indicated in the output.

```
Brocade(config-if-e1000-1/1)# show interfaces
GigabitEthernet1/1 is down, line protocol is down
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is GigabitEthernet, address is 0000.0034.5060 (bia 0000.0034.5060)
  Configured speed auto, actual unknown, configured duplex fdx, actual unknown
  Member of VLAN 1 (untagged), port is in untagged mode, port state is Disabled
  STP configured to ON, Priority is level0, flow control enabled
  OpenFlow enabled, Openflow Index 1, Flow Type Layer2
```

```
Priority force disabled, Drop precedence level 0, Drop precedence force disabled
dhcp-snooping-trust configured to OFF
```

Displaying the configured connections to controllers

Use the **show openflow** command to display the OpenFlow configuration, including the configured connections to controllers on the device.

```
Brocade(config)# show openflow
Administrative Status:      Enabled
Controller Type:            OFV 100
Number of Controllers:      3
Controller 1:
Connection Mode:            active, TCP
Controller Address:         10.25.128.243
Connection Port:            6633
Controller 2:
Connection Mode:            active, TCP
Controller Address:         10.25.128.242
Connection Port:            6633
Controller 3:
Connection Mode:            passive, TCP
Listening Address:          0.0.0.0
Connection Port:            6633

Match Capabilty:
Port, Destination MAC, Vlan, Vlan PCP
Openflow Enabled Ports:     e1/1 e1/2
```

TABLE 8   Output fields for the show openflow command

Field	Description
Administrative Status	Indicates the administrative status of OpenFlow on the device.
Controller Type	Indicates the OpenFlow protocol version that is supported on the device. Currently, Brocade devices support OpenFlow version 1.0.0.
Number of controllers	Lists the number of controller connections configured on the device. Brocade devices support up to three concurrent controller connections.
Connection Mode	Indicates the mode of the controller connection configured. You can configure active or passive connection to controllers. An active connection is initiated by the device. In a passive connection, the device is in the listening mode, and accepts requests from controllers. If the optional controller address is not specified, any controller can establish a connection with the device in the passive mode. See "Connecting to an OpenFlow controller".
Controller Address	Indicates the address of the specified controller.
Connection Port	Indicates the TCP port that is used for connection to the controller. By default, port 6633 is used.
Match Capability	Specifies the matching rules supported.
OpenFlow Enabled Ports	Lists the ports on the device that are enabled for OpenFlow.

Displaying the data path ID of the device

OpenFlow associates a globally unique data path ID to be used by the controller to distinguish OpenFlow devices on a network. To display the data path ID assigned to the device, enter the following command:

```
Brocade(config)# openflow datapath-id
"0000001bedb3d0c0"
```

Syntax: openflow datapath-id

Displaying the OpenFlow flows

You can display the OpenFlow flows that are configured on the device and their statistics. Enter the following command:

```
Brocade(config)# show openflow flows eth 1/2
```

Syntax: show openflow flows [eth x/y] [flowid]

The **show openflow flows** command shows all the flows configured in the system flow table. If you specify the interface, all the flows configured in the system for that interface are displayed. You can specify the optional **flowid** keyword to display the flows configured in the system and associated with the specified flow ID.

NOTE
On the Brocade NetIron CER and Brocade NetIron CES devices, statistics are available only for up to 2048 flows on a first-come-first-served basis.

```
Brocade(config)# show openflow flows
Total Number of Flows:                    2
Total number of data packets sent to controller:  0
```

```
Total number of data bytes sent to controller:     0
Flow ID: 1 Priority: 32768 Status: Active
      Rule:
          In Port: e1/2
          In Vlan: Untagged
          Destinaltion Mac: 000.0000.0001
          Destination Mac Mask:FFFF.FFFF.FFFF
      Action: FORWARD
          Out Port: e1/1, Untagged
      Statistics: 0
          Total Pkts:  0
          Total Bytes: 0

Flow ID: 2 Priority: 32768 Status: Active
      Rule:
          In Port:        e1/2
          In Vlan:        Tagged [10]
          Vlan PCP:       4
          Destinaltion Mac:    0000.0000.0001
          Destination Mac Mask:FFFF.FFFF.FFFF
      Action: FORWARD
          Out Port: e1/1, Untagged
          Out Port: e1/3, Untagged
      Statistics: 0
          Total Pkts:  0
          Total Bytes: 0
```

TABLE 9   Output fields for the show openflow flows command

Field	Description
Total Number of Flows	The total number of flows on the device.
Total number of data packets sent to controller	The number of packets sent to the controller.
Total number of data byte sent to controller	The number of bytes sent to the controller.
Flow ID	An identifier for each flow. You can use the flow ID from this output to display flow-specific details.
Priority	The priority of the flow set by the controller when the flow is added, in the range 0 to 65536. If the priority value was not specified, the Brocade device will assign the default value, 32768.
Status	Indicates whether the flow is configured correctly in the device. A correctly configured flow will have its status as ACTIVE.
Rule	Specifies the matching rule for the flow. In this example, the matching rule is for the flow with Flow ID 1, to forward untagged packets reaching the interface eth 1/2 with the destination MAC address of 0000.0000.0001, to the egress port eth 1/1 as untagged packets. Here, the destination MAC Address Mask of FFFF.FFFF.FFFF indicates that only packets exactly matching the specified destination MAC address will be forwarded.
Statistics	Indicates the counter of packets and bytes. For Brocade NetIron CER and Brocade NetIron CES devices, only the number of packets will be displayed.

OpenFlow scaling

- Switchover and HLOS are not supported. When the active management processor (MP) goes down, communication with the controller is brought down and the flow tables on the MP and all line processors (LP) are cleared. The connection with the controller is re-established after switchover.

- When LP is reset, the flow table on the LP is restored once the LP comes up and flows specific to that LP are maintained in the MP.

- When an OpenFlow-enabled port goes up or down, no rules are removed. The addition or deletion of rules depends solely on the controller.

- Brocade NetIron CER devices support 32K OpenFlow entries and Brocade NetIron CES devices support 4K OpenFlow entries only. Brocade MLX Series and Brocade NetIron XMR devices support 64K and 128K OpenFlow entries respectively.

- Up to 2K protected VLANs per system are supported.

Administrating OpenFlow

Clearing the OpenFlow statistics

You can clear the flow statistics for all flows or, optionally for a specified flow. Only the counters of packets and bytes (when applicable) are cleared; none of the other flow table entries are affected.

To clear flow counters, enter the following command:

```
Brocade(config)#clear statistics openflow
```

Syntax: clear statistics openflow [flow-id]

The **flow-id** keyword, if specified, clears only the counters for the specified flow. Use the **show openflow flows** command to obtain flow IDs.

Deleting the OpenFlow flows

When an OpenFlow rule or all flows in the flow table need to be deleted you can use the **clear openflow flowid/all** *flow-id* command. Use this command to delete a single OpenFlow rule based on a flow-id or delete all flows in the flow table.

```
Brocade# clear openflow flowid 6
Brocade# clear openflow all
```

Syntax: clear openflow flowid |all *flow-id*

The **flowid** will delete a single OpenFlow rule with the given flow-id and **all** will delete all flows in the flow table.. The command will delete the rule irrespective of the state it is in (ACTIVE, PENDING_ADD, PENDING_MODIFY, PENDING_DELETE). The same rule can be added again later from the controller if needed.

Show tech

The **show tech-support openflow** command captures the output of multiple show commands at one time, tobe used for diagnostic purposes.

Brocade# `show tech-support openflow`.

Syntax: **show tech-support openflow**

This command will now capture the output of the following commands:

- show openflow datapath-id
- show openflow controller
- show openflow interface
- show openflow flows
- show versions
- show interfaces
- show statistics
- show running-config
- show logging
- show save

Example

TABLE 10   Output fields for the show openflow command

Field	Description
Administrative Status	Indicates the administrative status of OpenFlow on the device.
Controller Type	Indicates the OpenFlow protocol version that is supported on the device. Currently, Brocade devices support OpenFlow version 1.0.0.
Number of controllers	Indicates the number of controller connections configured on the device. Brocade devices support up to three concurrent controller connections.
Connection Mode	Indicates the mode of the controller connection configured. You can configure active or passive connection to controllers. An active connection is initiated by the device. In a passive connection, the device is in the listening mode, and accepts requests from controllers. If the optional controller address is not specified, any controller can establish a connection with the device in the passive mode.
Controller Address	Indicates the address of the specified controller.
Connection Port	Indicates the TCP port that is used for connection to the controller. By default, port 6633 is used.
Match Capability	Specifies the matching capabilities valid for the mode (Layer 2 or Layer 3). The matching capabilities include source port, source or destination MAC addresses, VLAN ID, and VLAN priority.
OpenFlow Enabled Ports	Indicates the ports on the device that are enabled for OpenFlow.
OpenFlow Hybrid Mode Ports	Indicates the VLAN ids.
Default Action	Indicates the default action for packets that do not match any configured flows. By default, such packets are dropped. However, you can configure these packets to be sent to the controller by using the **openflow default send-to-controller** command.
Maximum Number of Flows Allowed	Indicates the maximum number of flows allowed on the device that is configured by using the **system-max openflow-flow-entries** command.

OpenFlow configuration considerations

After you enable OpenFlow on a device, you can configure, generate, and monitor flows on the ports configured on the device from a controller on OpenFlow-enabled ports. The Brocade device flow table is entirely under the control of the OpenFlow Controller. Keep in mind the following when you configure and monitor OpenFlow features on the devices:

Behavior of ports and devices

- Ports that are enabled for OpenFlow cannot take part in any of the normal operations of the device, such as routing and L2 forwarding. However, after OpenFlow is disabled on a port, the port can resume normal operations. This does not require disabling OpenFlow globally on the device.

- OpenFlow defines port numbers sequentially from 1. The `OF-portid` parameter in the output of the **show openflow interface** command is assigned to the ports on the device. On Brocade MLX Series and Brocade NetIron XMR devices, 48 OpenFlow ports are reserved per slot. OpenFlow port numbering starts from slot 1. That is, OpenFlow port 1 is port 1/1 (1/1 = slot 1/port 1), OpenFlow port 2 is port 1/2, and so on. Therefore, slot 1 has OpenFlow ports 1-48, slot 2 has OpenFlow ports 49-96, and so on.

  For example, if slot 1 is an 8x10G card and slot 2 is an 8x10G card, then the OpenFlow ports will be: slot 1 (OpenFlow ports 1 to 8); slot 2 (OpenFlow ports 49 to 56). On Brocade NetIron CER and Brocade NetIron CES devices, ports 1/1 to 1/48 are OpenFlow ports 1 to 48 and ports 2/1 and 2/2 are OpenFlow ports 49 and 50. The OpenFlow protocol offers a capability discovery message for the controller to discover the ports that are OpenFlow-enabled on the router and their capabilities.

- The flow table content is not cleared when the connection to a controller is lost. The device will continue to forward traffic according to the flow entries defined in the flow table even in the absence of a controller connection.

- The flow table entries within the device are cleared when the device is reset.

- On the Brocade MLX Series and Brocade NetIron XMR devices, when the active management module in the device switches over, all controller connections are closed. Configured controller connections are reestablished after the device switches over to the standby management module.

- Flow table entries associated with a port are maintained when a port goes down. When the port comes back up, those flow entries are restored on the port. Flow entries are removed only with an explicit command from the controller.

- When OpenFlow is disabled globally on the device using the **no openflow enable** command, the flow table in the device is cleared. However, before you can disable OpenFlow globally on the device, you must disable OpenFlow on all interfaces individually.

- When a controller tries to add a flow to the device with the same priority, rule, and action as a flow that exists in the flow table, the flow statistics are cleared (the system does not add a new flow). The following table summarizes the behavior for similar flows being successively added:

TABLE 11 Flow table behavior when flows similar to existing ones are added

Priority	Rule	Action	Device behavior
Same	Same	Same	Clear flow statistics
Same	Same	Different	• Update the action list • Clear the statistics
Same	Different	Same	Create new flow
Same	Different	Different	Create new flow
Different	Same	Same	Create new flow
Different	Same	Different	Create new flow

Removing OpenFlow configuration from a device

In general, to remove OpenFlow from the device and make it a non-OpenFlow device, do the following:

1. Disable OpenFlow on the ports where it is enabled.

2. Disable OpenFlow on the device globally.

3. Optional: Set the maximum number of flows to zero using the **system-max openflow-flow-entries 0** command.

4. Reload the device.

Commands

The following commands support the features described in this chapter:

- openflow enable layer2|layer3 |layer23 hybrid-mode
- clear openflow flowid | all

openflow enable layer2|layer3 |layer23 hybrid-mode

Enables or disables the hybrid port mode on the port.

Syntax [no] openflow enable layer2|layer3 | layer23 hybrid-mode

Parameters *slot/port*   Specifies the port that you want to enable or disable the hybrid port mode.

Command Modes User EXEC mode
Privileged EXEC mode
Global configuration mode

Usage Guidelines The **show OpenFlow** command displays the configuration for OpenFlow and gives the information about hybrid mode port, protected VLAN ids and maximum number of protected VLANs allowed.

```
Brocade(config)# show openflow

Administrative Status:        Enabled
SSL Status:                   Enabled

Controller Type:              OFV 100
Number of Controllers:        1

Controller 1:
Connection Mode:        passive, TCP,
Listening Address:      0.0.0.0
Connection Port:        6633
Connection Status:       TCP_LISTENING

Match Capability:
L2 : Port, Source MAC, Destination MAC, Ether type, Vlan, Vlan PCP
L3 : Port, Vlan, Vlan PCP, Ethertype(IP,ARP,LLDP), Source IP, Destination IP, IP
Protocol, IP TOS, IP Src Port, IP Dst Port
L23: All

Normal Openflow Enabled Ports:
Openflow Hybrid Interfaces:
e1/1
Protected VLANs   : None
Unprotected VLANs :     2, 3, 4, 5, 6, 7, 8, 9, 10, 11
......................................................
......................................................
3994, 3995, 3996, 3997, 3998, 3999, 4000, 4001, 4011,

e2/1
Protected VLANs   : None
Unprotected VLANs :  4010,

Default action: drop
Maximum number of flows allowed: 65536
Active flow: 0

Maximum number of Protected Vlans allowed: 2048
Maximum number of Unprotected Vlans allowed: 4096
Total number of Unprotected Vlans: 4002
```

History

Release	Command History
Multi-Service IronWare R05.6.00	This command was modifed to display OpenFlow hybrid port mode information.

clear openflow flowid | all

Delete flows from the flow table.

Syntax   clear openflow flowid|all *flow-id*

Parameters   Flow ID   Clears the given flow-id that you want to delete from the flow table

.all   Deletes all flows from the flow table

**Command
Modes**   User EXEC mode
Privileged EXEC mode
Global configuration mode

**Usage
Guidelines**   When an OpenFlow rule or all flows in the flow table need to be deleted you can use the **clear
openflow flowid/all** *flow-id* command. Use this command to delete a single OpenFlow rule based
on a flow-id or delete all flows in the flow table.

```
Brocade# clear openflow flowid 6
Brocade# clear openflow all
```

History

Release	Command History
*Multi-Service IronWare
R05.5.00C*	This command was modifed to delete single flow on given flow-id or all flow deletion in the flow table.