# Brocade MLX Series and NetIron Family

## Documentation Updates

**Supporting Multi-Service IronWare R05.5.xx**

**BROCADE**

## Brocade Communications Systems, Incorporated

## Document History

| Title | Publication number | Summary of changes | Date |
| --- | --- | --- | --- |
| *Brocade MLX Series and NetIron Family Documentation Updates* | 53-1003096-01 | New document. | 11 October 2013 |
| *Brocade MLX Series and NetIron Family Documentation Updates* | 53-1003096-02 | Added defect correction in the Hardware Installation chapter. | 18 November 2013 |
| *Brocade MLX Series and NetIron Family Documentation Updates* | 53-1003096-03 | Updated for the R05.5.00e release. | 8 January 2014 |
| *Brocade MLX Series and NetIron Family Documentation Updates* | 53-1003096-04 | Updated with hardware information. | 27 February 2014 |

# Contents

**Chapter 2**    **Documentation Updates for the Unified IP MIB Reference**

**Chapter 3**    **Documentation Updates for the MLXe / MLX Series and NetIron XMR Series Hardware Installation Guides**

# About This Document

## In this chapter

- *"How this document is organized"* on page ix
- *"Brocade resources"* on page x
- *"Getting technical help"* on page x
- *"Document feedback"* on page x

## How this document is organized

This document contains updates to the Multi-Service IronWare R05.5.xx product manuals. These updates include document fixes and changes covering new features. Table 1 below list the most recently released Multi-Service IronWare R05.5.xx product manuals.

**TABLE 1**    Documentation supporting Multi-Service IronWare R05.5.xx

| Publication Title | Fabric OS Release | Page Number | Publication Date |
|---|---|---|---|
| *Multi-Service IronWare Administration Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare Multiprotocol Label Switch (MPLS) Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare IP Multicast Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare Routing Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare Software Defined Networking (SDN) Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare Security Configuration Guide* | R05.5.00c and later | Updates on page 1. | July 2013 |
| *Multi-Service IronWare Switching Configuration Guide* | | Updates on page 1. | July 2013 |
| *Multi-Service IronWare QoS and Traffic Management Configuration Guide* | | Updates on page 1. | July 2013 |
| *Brocade MLXe Series Hardware Installation Guide* | R05.5.00c and later | Updates on page 23 | September 2013 |
| *Brocade MLX Series and NetIron XMR Hardware Installation Guide* | R05.5.00c and later | Updates on page 23 | September 2013 |
| *Brocade NetIron CES Series and NetIron CER Series Hardware Installation Guide* | R05.5.00c and later | Updates on page 23 | September 2013 |
| *Multi-Service IronWare Software Upgrade Guide* | R05.5.00c and later | No Updates | July 2013 |
| *Brocade MLX Series and NetIron XMR Diagnostics Guide* | R05.5.00c and later | No Updates | July 2013 |
| *Unified IP MIB Reference* | R05.5.00c and later | Updates on page 19 | July 2013 |
| *Brocade MLX Series and NetIron XMR YANG Guide* | R05.5.00c and later | No Updates | July 2013 |

# Brocade resources

For the latest documentation, go to [http://www.brocade.com/ethernetproducts](http://www.brocade.com/ethernetproducts)

# Getting technical help

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

# Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback by email to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

# Documentation Updates for the Brocade MLX Series and NetIron Family Configuration Guide

## In this chapter

The updates in this chapter are for the following Configuration guides.

- Administration Configuration Guide - publication number 53-1002818-02
- Switching Configuration Guide - publication number 53-1002820-02
- Routing Configuration guide - publication number 53-1002821-02
- Multiprotocol Label Switch (MPLS) Configuration Guide - publication number 53-1002824-02
- IP Multicast Configuration Guide - publication number 563-1002823-02
- Security Configuration Guide - publication number 53-1002818-02
- QoS and Traffic Management Configuration Guide - publication number 53-1002822-02
- Software Defined Networking Guide - publication number 53-1002825-01

The following features were added or modified as part of the 5.5.00d release.

The following features were added or modified as part of the 5.5.00e release.

# IPv6 ND Router Advertisement Control

IPv6 ND Router Advertisement Control allows for disabling sending out router advertisements at the interface level. The **no ipv6 nd suppress-ra** command at the interface level allows the user to disable and enable the sending of the ND Router Advertisement on an interface. By default, the sending of ND Router Advertisement (RA) is enabled on all interfaces, except for the tunnel and loopback interfaces, providing that the IPv6 Unicast Routing is enabled and the interfaces are active for IPv6.

The IPv6 ND Router Advertisement Control gives the ability to quickly turn off the sending of IPv6 ND Router Advertisement message on an IPv6 enabled interfaces.

By default,

- The ND Router Advertisement is enabled.
- Interface is enabled to send ND Router Advertisements.
- The **ipv6 nd suppress-ra** and **ipv6 nd send-ra** interface commands, when configured, override the system and VRF global **ipv6 nd global-suppress-ra** command.

Users sometimes require the ability to quickly turn off the sending of IPv6 ND Router Advertisement message on an IPv6 enabled interfaces. This is achieved by providing the following additional configuration command at interface level:

```
Brocade(config-if-e10000-1/1)#no ipv6 nd suppress-ra
```

The **ipv6 nd send-ra** command is a new interface level command added as part of this enhancement. This allows the user to configure the sending of RA messages on some selected interfaces when the **ipv6 nd global-suppress-ra** command is set to disable the sending of RA messages on all other interfaces.

**Syntax: [no]ipv6 nd suppress-ra**

# MSTP

The following updates apply to the "MSTP support for PBB" in the STP chapter of the Switching guide.

The following limitation has been removed:

- Under MSTP topic, we need to create another section at the last as below

The following section has been added:

## High availability

MSTP supports MP switchover and hitless software upgrade. When an MSTP root bridge undergoes MP switchover and hitless upgrade, there will be no break in transmission of the MSTP BPDU during reboot of the line cards. Due to this, there will be no re-convergence of the topology and no disruption in traffic.

MSTP PBB with multi region feature also supports MP switchover and hitless software upgrade. There will be no traffic disruption during a hitless upgrade.

# MSTP support for PBB

The following configuration consideration has been added.

MSTP should not be configured for:

- topology groups having L2 member vlans
- member vlans configured in a topology group. A

If a topology group is configured with a master vlan running MSTP, layer 2 (L2) VLANs should not be configured as members until MSTP is disabled on the master VLAN of this topology group. Such configurations via CLI are blocked.

# VRRP and VRRP-E VRIDs

The following configuration consideration has been added to the VRRP chapter.

**NOTE**
With VRRP or VRRP-E the maximum numbers of VRIDs per logical interface is 12.

# Data Integrity Protection for Metro

The following section is an update to the Data Integrity Protection section of Chapter 3 in the NetIron 5.4.00 Configuration Guide.

**TABLE 1**  Feature support table

| 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 |
|---|---|---|---|---|---|---|---|
| Data Integrity Protection for Metro - Phase 2 | No | No | Yes | Yes | Yes | Yes | Yes |

Data Integrity Protection for Metro for Phase 2 introduces the ability to monitor low level memory corruption events occuring at the external Control Static Random Access Memory (CSRAM) in both Brocade NetIron CER and Brocade NetIron CES. Additionally, monitoring of the Longest Prefix Match (LPM) Memories are included as part of this feature.

There are a total of four LPM memories in total (LPM-0 to LPM-3). Brocade NetIron CER devices uses LPM-0 to LPM-2, which are on external memory chip. Brocade NetIron CES devices use LPM-3 only, which is internal. Brocade NetIron CES devices do not have external LPM memories.

Rolling windows are maintained for each of the monitor points. When any of the monitor points cross their configured thresholds SYSLOGs and traps are generated.

The CSRAM is used to store control tables and data structures in both Brocade NetIron CER and Brocade NetIron CES devices for extended capacity. The tables reside in an external DDR II/II + SRAM with a 36-bit data bus and are accessed by various engines in PPCR. The following are some tables/data structures stored in CSRAM.

- FDB Table and FDB Hash Table (MAC Table)
- DIT Data Structures (Down Stream Table)
- External INLIF Table (Interface Attributes)
- Ingress Policy Action Table
- Egress Policy Action Table
- IP/MPLS Next Hop Table
- TTI Engine Action Table

Brocade NetIron CER devices have three LPM Memories. The memories are 19-bit DDR II SRAMs. These memories hold the following data structures:

- IP Prefix Trees (for IP forwarding
- MPLS Interfaces (for MPLS LSR switching

Data Integrity Protection for Metro for Phase 2 extends the already existing Data Protection feature for Ingress and Egress data buffers to include the CSRAM and the LPM memories. Rolling windows are maintained for each of the monitor points. When any of the monitor points cross their configured threshold, SYSLOGs and traps are generated accordingly.

# Configuring Data Integrity Protection for Metro

1. Configure the Global Rolling Window Time Frame.

2. Configure the threshold parameters for CSRAM and/or LPM memories.

# Configuration commands

The following configuration commands are introduced to configure various parameters.

The **system np control-ram-threshold** command configures the CSRAM error reporting threshold.

```
Brocade(config)# system np control-ram-threshold 20
```

Syntax:  [no] **system np control-ram-threshold** *threshold*

The threshold range is 0 - 120 events. The default is 10 events. A value of 0 disables the monitoring.

The **[no]** option resets the threshold to default.

The **system np lpm-ram-threshold** command configures the LPM error reporting threshold.

```
Brocade(config)# system np control-ram-threshold 20
```

Syntax:  [no] **system np lpm-ram-threshold** *threshold*

The threshold range is 0 - 120 events. The default is 10 events. A value of 0 disables the monitoring.

The **[no]** option resets the threshold to default.

# Show commands

The following show commands have been added to the feature.

## *show np control-ram-errors*

The **show np control-ram-errors** command displays the Control RAM error event counter.

```
CSRAM
Ports            Current Cumulative
1/1  - 1/24           0          3
2/1  - 2/2            0          0
```

## *show np lpm-ram-errors*

The **show np lpm-ram-errors** command displays the LPM RAM error event counter.

```
                        LPM 0                  LPM 1                  LPM 2
Ports            Current Cumulative     Current Cumulative     Current Cumulative
1/1  - 1/24         0        3             0        3             0        3
2/1  - 2/2          0        3             0        3             0        3
```

## Syslog messages

The following are examples of Syslog messages that may be displayed.

```
NP CSRAM has 4 error events, exceeding configured threshold for interfaces 1/1 to
1/24.

NP LPM 1 has 4 error events, exceeding configured threshold for interfaces 1/1 to
1/24.
```

# RPF

## Configuration considerations for RPF

The following configuration consideration has changed.

The item stating Brocade MLX series and Brocade NetIron XMR devices do not support uRPF for VE interfaces is incorrect. The following configuation consideration replaces the incorrect information.

- RPF can only be configured at the physical port level. It should not be configured on virtual interfaces on the Brocade MLX series and Brocade NetIron XMR.
- Brocade MLX series and Brocade NetIron XMR devices support uRPF for VE interfaces, but they must be configured at the physical port level.

# Keep-alive VLAN

The following configuration consideration has been added.

**NOTE**
A port in keep-alive-vlan cannot be assigned to another VLAN.

# Configuring FDP

The following section describes how to enable FDP and how to change the FDP update and hold timers.

### *Enabling FDP globally*

To enable a Brocade device to globally send FDP packets, enter the following command at the global CONFIG level of the CLI.

```
Brocade(config)# fdp run
```

The feature is disabled by default.

**NOTE**
If FDP is globally enabled on a Brocade device, all the interfaces by default, will have FDP enabled on it. In this case, the **show run** command will not display any running information about the FDP configuration in its output.

## *Enabling FDP at the interface level*

You can enable FDP at the interface level by entering the following commands.

```
Brocade(config)# int e2/1
Brocade(config-if-e10000-2/1)# fdp enable
```

Syntax: [no] **fdp enable**

By default, the feature is enabled on an interface once FDP is enabled on the device. It is not enabled globally.

**NOTE**
To remove an interface from the global configuration, run the **no fdp enable** command in the interface mode explicitly. In this case, the **show run** displays the running configuration information for the specific interface at that instance.

**NOTE**
By removing FDP from the configuration, the **no fdp enable** stays in the configuration of the VPLS endpoint, which cannot be removed.

**NOTE**
FDP is not supported on VPLS/VLL endpoints.

# Enabling interception of CDP packets globally

To enable the device to intercept and display CDP packets, enter the following command at the global CONFIG level of the CLI.

```
Brocade(config)# cdp run
```

Syntax: [no] **cdp run**

The feature is disabled by default.

**NOTE**
If CDP is globally on a Brocade device, all of the interfaces, by default, will have CDP enabled on it. In this case, the **show run** will not display any running information about CDP configuration in its output.

## *Enabling interception of CDP packets on an interface*

You can disable and enable CDP at the interface level.

You can enter the following commands.

```
Brocade(config)# int e2/1
```

```
Brocade(config-if-e10000-2/1)# cdp enable
```

**Syntax: [no] cdp enable**

By default, the feature is enabled on an interface on CDP is enabled on the device.

**NOTE**
To remove an interface from the global CDP configuration, run the **no cdp enable** command in the interface mode explicitly. In this case, the **show run** displays the running configuration information for the specific interface at that instance.

**NOTE**
By removing FDP from the configuration, the **no cdp enable** stays in the configuration of the VPLS endpoint, which cannot be removed.

**NOTE**
CDP is not supported on VPLS/VLL endpoints.

# Configuring VPLS endpoint over FDP/CDP interface

Configuring VPLS endpoint over a FDP/CDP enabled interface will implicitly disable the FDP/CDP configuration on that specific interface for that instance, considering FDP/CDP is enabled globally. In this case, the **shop run** command will display the running configuration information as shown below.

The following examples explains the **show run** output for different instances:

- The **show run** output when the VPLS endpoint is configured over a globally enabled FDP/CDP interface:

```
Brocade(config-mpls-vpls-svlan-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
FDP/CDP is disabled on port 4/3
FDP/CDP is disabled on port 4/5
FDP/CDP is disabled on port 4/7
```

- The **show run** output when the VPLS endpoint is configured over a globally enabled FDP/CDP interface:

```
Brocade(config-mpls-vpls-svlan-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
FDP/CDP is disabled on port 4/3
FDP/CDP is disabled on port 4/5
FDP/CDP is disabled on port 4/7
```

- The **show run** output when the VPLS output is removed over a globally enabled FDP/CDP interface:

```
FDP/CDP is enabled on port 4/3
FDP/CDP is enabled on port 4/5
FDP/CDP is enabled on port 4/7
```

- The **show run** output when the VPLS endpoint is removed over a globally enabled FDP/CDP interface:

```
FDP/CDP is enabled on port 4/3
FDP/CDP is enabled on port 4/5
FDP/CDP is enabled on port 4/7
```

**NOTE**
If an VPLS endpoint is configured over a globally enabled FDP/CDP interface, the show run will not display FDP/CDP information for that specific interface until the VPLS endpoint is deleted. On deleting the VPLS endpoints, the previous FDP/CDP configuration is retained over that specific interface and the show run displays the FDP/CDP information again for that interface.

**NOTE**
By removing the FDP/CDP from the configuration, the **no cdp enable** or **no fdp enable** stays in the configuration of the VPLS endpoint, both of which cannot be removed.

# Configuring VLL endpoint over FDP/CDP enabled interface

Configuring VLL endpoint over an FDP/CDP enabled interface will implicitly disable the FDP/CDP configuration and also will be enable back implicitly when the VLL endpoint is deleted on that specific interface, considering the FDP/CDP is enabled globally.

Information messages will be displayed to notify the user as below in these cases:

For example, when VLL endpoint is created, the information messages are as below.

1. When only FDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

2. When only CDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

3. When both FDP/CDP are enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

For example, when the VLL endpoint is deleted the information messages are displayed as below.

1. When only FDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan -100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP is enabled on port 4/3
info - FDP is enabled on port 4/5
info - FDP is enabled on port 4/7
```

2. When only CDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP is enabled on port 4/3
```

```
        info - FDP is enabled on port 4/5
        info - FDP is enabled on port 4/7
```

3.  When both FDP/CDP are enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP/CDP is enabled on port 4/3
info - FDP/CDP is enabled on port 4/5
info - FDP/CDP is enabled on port 4/7
```

**NOTE**
If the VLL endpoint is configured over a globally enabled FDP/CDP interface, the show run command does not display the FDP/CDP information for that specific interface.

**NOTE**
By removing FDP/CDP from the configuration, the **no fdp enable** and **no cdp enable** stays in the configuration of the VPLS endpoints, which cannot be removed.

# Configuration considerations

The following configuration consideration is modified in the sFlow chapter of the Switching Configuration Guide.

**NOTE**
Interface module processors directly forward sFlow packets to the specified sFlow collector. The sFlow collector is reachable by the way of ports on any of the Interface modules. Brocade requires sFlow collector to be connected to non-management port.

# PIM over MCT

The MCT feature interaction matrix has been updated to indicate that BFD is not supported in NetIron 5.5.00 and later releases.

## MCT feature interaction

Use the following feature matrix when configuring MCT:

MCT feature interaction matrix

| Supported | Not Supported |
|---|---|
| **BGP**, **IS-IS**, and **OSPF** on CCEP. | **BFD** on CCEP. |

# Multicast snooping over MCT

The following configuration consideration is modified in the *Configuration considerations* list under the *Multicast snooping over MCT* section of the Multi-Chassis Trunking (MCT) chapter.

- On Customer Client Edge Ports (CCEP), MCT does not support 802.1ah.

# HQoS Feature support

The following features are supported in NetIron 5.5.00. The following documentation supplements the Multi-Service IronWare QoS and Traffic Management Configuration Guide.

**TABLE 2**    Supported platforms

| 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 |
|---|---|---|---|---|---|---|---|
| HQoS for VPLS | Yes | Yes | No | No | No | No | No |
| HQoS over LAG | Yes | Yes | No | No | No | No | No |
| WRED support for HQoS | Yes | Yes | No | No | No | No | No |

# HQoS for VPLS traffic overview

This feature allows you to support HQoS for VPLS traffic, where the traffic could be to or from the VPLS cloud. The HQoS map is applied on the MPLS uplink. Traffic coming from a VPLS end-point and going out of the MPLS uplink will be processed for HQoS.

## Feature highlights

HQoS was previously supported for "local VPLS" only. This feature is an enhancement to allow HQoS for VPLS in addition to local VPLS. A new match condition containing the VPLS ID and the VPLS Peer IP address has been added to the HQoS map command.

## Configuring HQoS for VPLS traffic

These steps assume the following topology:

- PE11 and PE12 routers are MCT nodes
- PE3 (1.1.1.2) is the remote PE router
- PE11 and PE12 are connected through MPLS

1. Use the following commands to configure HQoS policy on Node PE11

```
Brocade (config)# HQOS scheduler-policy policy-1 level level-0
Brocade (config-hqos-scheduler-policy policy-1)# shaper-rate 1000000
Brocade (config-hqos-scheduler-policy policy-1)# shaper-burst-size 128
Brocade (config-hqos-scheduler-policy policy-1)# scheduler-type strict
Brocade (config-hqos-scheduler-policy policy-1)# scheduler-flow flow-1-0
scheduler- input 0 scheduler-policy policy-2
Brocade (config-hqos-scheduler-policy policy-1)# scheduler-flow flow-1-1
scheduler- input 1 scheduler-policy policy-2
Brocade (config-hqos-scheduler-policy policy-1)#!
Brocade (config-hqos-scheduler-policy policy-1)#HQOS scheduler-policy policy-2
leve l level-1
Brocade (config-hqos-scheduler-policy policy-2)# shaper-rate 1000000
Brocade (config-hqos-scheduler-policy policy-2)# shaper-burst-size 64
Brocade (config-hqos-scheduler-policy policy-2)# scheduler-type strict
Brocade (config-hqos-scheduler-policy policy-2)# scheduler-flow flow-2-0
scheduler- input 0 scheduler-policy policy-3
Brocade (config-hqos-scheduler-policy policy-2)# scheduler-flow flow-2-1
scheduler- input 1 scheduler-policy policy-3
Brocade (config-hqos-scheduler-policy policy-2)#
Brocade (config-hqos-scheduler-policy policy-2)#HQOS scheduler-policy policy-3
leve l level-2
Brocade (config-hqos-scheduler-policy policy-3)# shaper-rate 20000
Brocade (config-hqos-scheduler-policy policy-3)# shaper-burst-size 64
Brocade (config-hqos-scheduler-policy policy-3)# scheduler-type strict
Brocade (config-hqos-scheduler-policy policy-3)# scheduler-flow flow-3-0
scheduler- input 0 scheduler-policy policy-4
Brocade (config-hqos-scheduler-policy policy-3)# scheduler-flow flow-3-1
scheduler- input 1 scheduler-policy policy-4
Brocade (config-hqos-scheduler-policy policy-3)#!
Brocade (config-hqos-scheduler-policy policy-3)#HQOS scheduler-policy policy-4
leve l level-3
Brocade (config-hqos-scheduler-policy policy-4)# shaper-rate 2000
Brocade (config-hqos-scheduler-policy policy-4)# shaper-burst-size 10
Brocade (config-hqos-scheduler-policy policy-4)# scheduler-type strict
Brocade (config)#router mpls
Brocade (config-mpls)#mpls-interface e3/3
Brocade (config-mpls-if-e100-3/3)#mpls-interface ve 200
Brocade (config-mpls-if-ve-200)#
Brocade (config-mpls-if-ve-200)# vpls test1 5000
Brocade (config-mpls-vpls-test1)# vpls-peer 1.1.1.2
Brocade (config-mpls-vpls-test1)# vlan 100
Brocade (config-mpls-vpls-test1-vlan-100)# tagged ethe 4/1
```

2. Use the following commands to configure HQoS for VPLS on Node PE11

```
Brocade (config)# interface ethernet 3/3
Brocade (config-if-eth-3/3) # hqos service-policy output policy-1

Brocade (config-if-eth-3/3) # hqos-map flow-1-1.flow-2-1.flow-3-1 match vpls 5000
peer 1.1.1.2
Brocade (config-if-eth-3/3)# enable
```

## Limitations

- The same configuration must be applied on both MCT nodes.
- Any module (except **BR-MLX-10Gx24** and **BR-MLX-40Gx4-X**) can be used for ingress traffic destined for an HQoS port. Only **BR-MLX-10Gx8-M** and **BR-MLX-10Gx8-X** modules support egressing HQoS traffic.
- It is recommended that you configure the HQoS Map on all the MPLS Uplink interfaces.
- BGP Auto-discovery for VPLS is not supported.
- HQoS will not work properly in MCT VPLS failure scenario e.g. CCP-DOWN or Spoke Down.

## Checking for HQoS for VPLS configurations on ports

**Example 1:**

```
Brocade #show run int e 3/3
interface ethernet 3/3
hqos service-policy output policy-1
hqos-map flow-1-1.flow-2-1.flow-3-1 match vpls 5000 peer 1.1.1.2
enable
```

After a succesful configuration on PE11, the show command output indicates that HQoS will be applied to traffic coming from VPLS 5000 endpoint and going to VPLS peer 1.1.1.2 on the MPLS interface eth 3/3.

**Example 2:**

```
Brocade #show run int e 4/1
interface ethernet 4/1
hqos service-policy output policy-1
hqos-map flow-1-1.flow-2-1.flow-3-1 match vlan 100
enable
```

After a succesful configuration on PE11, the show command output indicates that HQoS will be applied to traffic coming from peer 1.1.1.2 and going to VPLS 5000 endpoint, interface eth 4/1.

# HQoS for LAG traffic overview

This feature allows you to support HQoS for LAG traffic, where the traffic could be to or from the VPLS cloud. The HQoS map is applied on the MPLS uplink. Traffic coming from a VPLS end-point that is part of a LAG, and going out of the MPLS uplink will be processed for HQoS.

## Feature highlights

HQoS over LAG is supported for VPLS Endpoint, Local VPLS, and MPLS VPLS Uplink.

- When LAG is undeployed, the HQos Configuration on the primary and all secondary ports will be retained.
- Addition of a new port to the LAG is allowed, if and only if, the HQoS Configuration of the newly added port is identical to that of the primary port of the deployed LAG.
- Removal of a port from the deployed LAG with HQoS configuration will retain the HQoS Configuration on the port which is being removed from the LAG.

- Before the HQoS configuration is applied on the primary port of a deployed LAG, and the configuration is replicated on all the secondary ports of the LAG, the following checks are made.
  - It is ensured that the resources are available (per TM).
  - All member ports are 8x10G ports that support HQoS when the policy is applied. Different kinds of 10G ports are not mixed.
  - If the member port list contains ports that are not HQoS capable, the CLI command flags an error and disallows the command execution.
  - When unbinding an HQoS policy from a port, HQoS policy is removed from all member ports and resources are de-allocated from all the member ports.

## Configuring steps

HQoS over LAG is configured under the primary port of the LAG.

1. Use this command to set up a LAG and Primary port

```
Brocade # lag "testLag" dynamic id 1
ports ethernet 4/3 to 4/5
primary-port 4/3
deploy
```

2. Use the following commands to configure HQoS on the primary port of the LAG

```
Brocade (config)# interface ethernet 4/3
Brocade (config-if-eth-4/3) # hqos service-policy output policy-1
Brocade (config-if-eth-4/3) # hqos-map flow-1-1.flow-2-1.flow-3-1 match vlan 200
(Existing VPLS End-point)
Brocade (config-if-eth-4/3) # hqos-map flow-1-1.flow-2-1.flow-3-0 match vpls 501
peer 1.1.1.2 (VPLS MPLS Uplink)
Brocade (config-if-eth-4/3)# enable
```

The HQoS configuration will be replicated on both the secondary ports (4/4, 4/5) of the LAG.Depending on the traffic patterns and the hash function used, lag hashing may result in non-uniform distribution of traffic to member ports. Each member port is individually capable of forwarding the traffic which is configured as part of the corresponding HQoS-policy and HQoS-map rule. The HQoS over LAG is supported both for the VPLS End-point & VPLS MPLS Uplink.

## Limitations

- All member ports need to have the same HQoS configuration before the LAG can be deployed. This condition covers the following cases.
  - No HQoS configuration exists on any member ports
  - HQoS configuration on all member ports is the same
  - If no HQoS configuration exists on any member ports, member ports with different capabilities (HQoS capable and non-HQoS capable) will be allowed.

# WRED support for HQoS

This feature allows you to support WRED for HQoS customer and other queue types.

## Feature highlights

This feature is implemented using enhancements to existing CLI commands for QoS on regular port queue types.

## Configuring steps

1.  Use the following commands to set up WRED on a 10G module and a customer-queue type.

```
Brocade # hqos customer-queue-type 0 wred enable module-type 8x10g
Brocade # hqos customer-queue-type 0 wred averaging-weight 1 module-type 8x10g
```

2.  Use the following commands to set up WRED on a 10G module and an other-queue type.

```
Brocade # hqos other-queue-type 7 wred enable module-type 8x10g
Brocade # hqos other-queue-type 7 wred drop-precedence 3 max-avg-queue-size 512
module-type 8x10g
```

Use the show command to check your configuration. After a successful configuration, the show command output will be similar to what is shown in the example below.

**Example 1:**

```
Brocade #show hqos wred module-type 8x10g
Other Traffic
QType Enable AverWeight MaxQSz DropPrec MinAvgQSz MaxAvgQSz MaxDropProb MaxPktSz
  0    No
  1    No
  2    No
  3    No
  4    No
  5    No
  6    No
  7    Yes    4(6.25%)    1024      0        1024      1088        0%        16384
                                    1        704       832         2%        16384
                                    2        448       832         5%        16384
                                    3        384       512         6%        16384
Customer Traffic
  0    Yes    1(50.0%)    1024      0        384       1024        2%        16384
                                    1        320       1024        4%        16384
                                    2        256       1024        9%        16384
                                    3        192       1024        10%       16384
  1    No
  2    No
  3    No
```

## Commands

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [**wred enable module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [ **wred averaging-weight** *avg-weight-value* **module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [ **wred drop-precedence** *drop-precedence-value* **max-avg-queue-size | min-avg-queue-size** *min-size | max-size* **module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [ **wred drop-precedence** *drop-precedence-value* **drop-probability-max** *p-max* **module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [ **wred drop-precedence** *drop-precedence-value* **packet-size-max** *pkt-size* **module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [**default-params module-type** *module-type*]

Syntax:  [no] hqos customer-queue-type | other-queue-type *queue-type* [**wred drop-precedence** *drop-precedence-value* **default-params module-type** *module-type*]

Syntax:  show hqos [**wred module-type** *module-type*]

# Configuring VPLS endpoint over FDP/CDP interface

Configuring VPLS endpoint over a FDP/CDP enabled interface will implicitly disable the FDP/CDP configuration on that specific interface for that instance, considering FDP/CDP is enabled globally. In this case, the **shop run** command will display the running configuration information as shown below.

The following examples explains the **show run** output for different instances:

- The **show run** output when the VPLS endpoint is configured over a globally enabled FDP/CDP interface:

```
Brocade(config-mpls-vpls-svlan-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
FDP/CDP is disabled on port 4/3
FDP/CDP is disabled on port 4/5
FDP/CDP is disabled on port 4/7
```

- The **show run** output when the VPLS endpoint is configured over a globally enabled FDP/CDP interface:

```
Brocade(config-mpls-vpls-svlan-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
FDP/CDP is disabled on port 4/3
FDP/CDP is disabled on port 4/5
FDP/CDP is disabled on port 4/7
```

- The **show run** output when the VPLS output is removed over a globally enabled FDP/CDP interface:

```
FDP/CDP is enabled on port 4/3
FDP/CDP is enabled on port 4/5
FDP/CDP is enabled on port 4/7
```

- The **show run** output when the VPLS endpoint is removed over a globally enabled FDP/CDP interface:

```
FDP/CDP is enabled on port 4/3
FDP/CDP is enabled on port 4/5
FDP/CDP is enabled on port 4/7
```

**NOTE**
If an VPLS endpoint is configured over a globally enabled FDP/CDP interface, the show run will not display FDP/CDP information for that specific interface until the VPLS endpoint is deleted. On deleting the VPLS endpoints, the previous FDP/CDP configuration is retained over that specific interface and the show run displays the FDP/CDP information again for that interface.

**NOTE**
By removing the FDP/CDP from the configuration, the **no cdp enable** or **no fdp enable** stays in the configuration of the VPLS endpoint, both of which cannot be removed.

# Configuring VLL endpoint over FDP/CDP enabled interface

Configuring VLL endpoint over an FDP/CDP enabled interface will implicitly disable the FDP/CDP configuration and also will be enable back implicitly when the VLL endpoint is deleted on that specific interface, considering the FDP/CDP is enabled globally.

Information messages will be displayed to notify the user as below in these cases:

For example, when VLL endpoint is created, the information messages are as below.

1. When only FDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

2. When only CDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

3. When both FDP/CDP are enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# tag eth 4/3 eth 4/5 eth 4/7
info- FDP is disabled on port 4/3
info- FDP is disabled on port 4/5
info- FDP is disabled on port 4/7
```

For example, when the VLL endpoint is deleted the information messages are displayed as below.

1. When only FDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan -100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP is enabled on port 4/3
info - FDP is enabled on port 4/5
info - FDP is enabled on port 4/7
```

2. When only CDP is enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP is enabled on port 4/3
info - FDP is enabled on port 4/5
info - FDP is enabled on port 4/7
```

3. When both FDP/CDP are enabled globally

```
Brocade(config-mpls-vll-vll1-vlan-100)# no tag eth 4/3 eth 4/5 eth 4/7
info - FDP/CDP is enabled on port 4/3
info - FDP/CDP is enabled on port 4/5
info - FDP/CDP is enabled on port 4/7
```

**NOTE**
If the VLL endpoint is configured over a globally enabled FDP/CDP interface, the show run command does not display the FDP/CDP information for that specific interface.

**NOTE**
By removing FDP/CDP from the configuration, the **no fdp enable** and **no cdp enable** stays in the configuration of the VPLS endpoints, which cannot be removed.

# Documentation Updates for the Unified IP MIB Reference

## In this chapter

The updates in this chapter are for the *Unified IP MIB Reference*, publication number 53-1002648-02, published June 2013.

-

## Agent board table

Updated snAgentBrdIndex (OID brcdIp.1.1.2.2.1.1.1) object index range from 1 through 42 in the snAgentBrdTable.

## brcdNPCSRAMErrorTable (to query for NP CSRAM errors)

The brcdNPCSRAMErrorTable displays information of Network Processor (NP) Control Static Random Access Memory (CSRAM) MIB objects.

**NOTE**
The following MIB objects are supported on the Brocade NetIron CES and Brocade NetIron CER devices.

| Name, OID, and syntax | Access | Description |
|---|---|---|
| brcdNPCSRAMErrorTable<br>brcdIp.1.14.2.1.1.4 | None | The table contains information of various Network Processor (NP) CSRAM error event counters supported by the system.<br>The objects in this table are refreshed every second, based on request.<br>This table is only supported on CES/CER. |
| brcdNPCSRAMErrorSlotId<br>brcdIp.1.14.2.1.1.4.1.1<br>Syntax: Unsigned32 | None | Slot-ID of the module that uniquely identifies it in the system. The module must be a UP and physically present. This is an 1-based index. |
| brcdNPCSRAMErrorDeviceId<br>brcdIp.1.14.2.1.1.4.1.2<br>Syntax: Unsigned32 | None | The Network Processor device-ID. A number that uniquely identifies the NP within a module in the system. This is an 1-based index. |
| brcdNPCSRAMErrorDescription<br>brcdIp.1.14.2.1.1.4.1.3<br>Syntax: DisplayString | Read-only | Details the range of ports serviced by the NP identified by brcdNPCSRAMErrorSlotId and brcdNPCSRAMErrorDeviceId objects. |

| Name, OID, and syntax | Access | Description |
|---|---|---|
| brcdNPCSRAMErrorCurrentEvents<br>brcdIp.1.14.2.1.1.4.1.4<br>Syntax: Counter32 | Read-only | Counter for NP CSRAM errors recorded within a configured window. |
| brcdNPCSRAMErrorCumulativeEvents<br>brcdIp.1.14.2.1.1.4.1.5<br>Syntax: Counter32 | Read-only | Counter for total NP CSRAM errors recorded. |

# brcdNPLPMRAMErrorTable (to query for NP LPM-RAM errors)

**NOTE**
The following MIB objects are supported only on the Brocade NetIron CES and Brocade NetIron CER devices.

| Name, OID, and syntax | Access | Description |
|---|---|---|
| brcdNPLPMRAMErrorTable<br>brcdIp.1.14.2.1.1.5 | None | A list of brcdNPLPMRAMError entries. The table contains information of various LPM RAM error event counters supported by the Network processor in the system. The objects in the table are refreshed every second, based on the request. |
| brcdNPLPMRAMErrorIndex<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: Unsigned32 | None | This object uniquely identifies a LPM within a Network Processor. Brocade NetIron CER devices use LPM-0, LPM-1 and LPM-2 memories, whereas Brocade NetIron CES devices use LPM-3 memory. This is an 1-based index.<br>Index value of 1 maps to LPM0, 2 maps to LPM1 and so on. |
| brcdNPLPMRAMErrorSlotId<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: Unsigned32 | None | Slot-ID of the module that is uniquely identifies it in the system. The module must be a UP and physically present. This is an 1-based index. |
| brcdNPLPMRAMErrorDeviceId<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: Unsigned32 | None | The Network Processor device-ID. A number that uniquely identifies the NP within a module in the system. This is an 1-based index. |
| brcdNPLPMRAMErrorName<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: DisplayString | Read-only | Details a string representing the LPM identified by brcdNPLPMRAMErrorIndex. |
| brcdNPLPMRAMErrorDescription<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: DisplayString | Read-only | Details the range of ports serviced by the NP identified by brcdNPLPMRAMErrorSlotId and brcdNPLPMRAMErrorDeviceId objects. |
| brcdNPLPMRAMErrorCurrentEvents<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: Counter32 | Read-only | Counter for the error events recorded within a configured window in the LPM identified by brcdNPLPMRAMErrorIndex, brcdNPLPMRAMErrorSlotId, and brcdNPLPMRAMErrorDeviceId objects. |
| brcdNPLPMRAMErrorCumulative Events<br>brcdIp.1.14.2.1.1.5.1.1<br>Syntax: Counter32 | Read-only | Counter for the error events recorded within a configured window in the LPM identified by brcdNPLPMRAMErrorIndex, brcdNPLPMRAMErrorSlotId, and brcdNPLPMRAMErrorDeviceId objects. |

# Traps

The following new traps are added to report the CSRAM and LPMRAM errors on the Brocade NetIron CES and Brocade NetIron CER devices.

| Trap name and number | Object ID | Severity | Description |
|---|---|---|---|
| brcdNPCSRAMErrorThresholdExceeded<br>brcdIp.1.14.2.0.3 | brcdNPCSRAMErrorDescription,<br>brcdNPCSRAMErrorCurrentEvents | Alerts | The SNMP trap that is generated when the Network Processor CSRAM error event count within a window exceeds the configured threshold.<br>Sample syslog message:<br>`NP CSRAM has 4 error events, exceeding configured threshold for interfaces 1/1 to 1/24.` |
| brcdNPLPMRAMErrorThreshold Exceeded<br>brcdIp.1.14.2.0.4 | brcdNPLPMRAMErrorName,<br>brcdNPLPMRAMErrorDescription,<br>brcdNPLPMRAMErrorCurrentEvents | Alerts | The SNMP trap that is generated when the Network Processor LPMRAM error event count within a window exceeds the configured threshold.<br>Sample syslog message:<br>`NP LPM 1 has 4 error events, exceeding configured threshold for interfaces 1/1 to 1/24.` |

**2**    brcdNPLPMRAMErrorTable (to query for NP LPM-RAM errors)

# Documentation Updates for the MLXe / MLX Series and NetIron XMR Series Hardware Installation Guides

## In this chapter

The updates in this chapter are for the following publications:

- Brocade NetIron CES and Brocade NetIron CER Devices Hardware Guide - publication number 53-0000080-03
- Brocade MLXe Series Hardware installation Guide - publication number 53-0000070-03
- Brocade MLX Series and Brocade NetIron XMR Series Hardware Installation Guide - publication number 53-0000040-04

## Switch fabric modules

### Brocade MLXe Series

The following table note is added to the "blinking" state of the switch fabric module LED in the Product Overview chapter of the Brocade MLXe Series Hardware Installation Guide.

**TABLE 1**  Switch fabric module LEDs

| LED | Position | State | Meaning |
|---|---|---|---|
| Pwr | Above Active LED | On | The module is receiving power. |
| | | Off | The module is not receiving power. |
| Active | Below Pwr LED | On (4-, 8-, and 16-slot routers only) | The switch fabric is on (active) and ready to switch user packets. |
| | | Blinking (32-slot routers only) | The switch fabric is on (active) and being accessed by the Management Module CPU. This indicates normal operation. <br><br> **NOTE:** On devices supporting software version R05.3.00 and earlier, when you insert an SFM or during powering on the device, the Active LED was off for a short duration, up to 15 seconds because the monitoring of the Fabric module is stopped for this duration. After this delay, the LED indicated the monitoring status. In version R05.4.00 and later, the Active LED reads the switch fabric continuously even during module insertion or powering on the device, and thus the Active LED blinks. |
| | | Off for extended period | The switch fabric is not active and cannot switch user packets. |

## Brocade MLX Series and Brocade NetIron XMR

The following table note is added to the "blinking" state of the switch fabric module LED in the Product Overview chapter of the Brocade MLX Series and Brocade NetIron XMR Series Hardware Installation Guide.

**TABLE 2**      Switch fabric module LEDs

| LED | Position | State | Meaning |
|---|---|---|---|
| Pwr | Above Active LED | On | The module is receiving power. |
| | | Off | The module is not receiving power. |
| Active | Below Pwr LED | On <br>(4-, 8-, and 16-slot routers only) | The switch fabric is on (active) and ready to switch user packets. |
| | | On <br>(32-slot routers only) | The switch fabric is on (active) and ready to switch user packets. |
| | | Blinking <br>(32-slot routers only) | The switch fabric is on (active) and being accessed by the Management Module CPU. This indicates normal operation. <br><br>**NOTE:** On devices supporting software version R05.3.00 and earlier, when you insert an SFM or during powering on the device, the Active LED was off for a short duration, up to 15 seconds because the monitoring of the Fabric module is stopped for this duration. After this delay, the LED indicated the monitoring status. In version R05.4.00 and later, the Active LED reads the switch fabric continuously even during module insertion or powering on the device, and thus the Active LED blinks. |
| | | Off for extended period | The switch fabric is not active and cannot switch user packets. |

# Cable specifications

The following caution has been added to Chapter 6 Connecting a Router to a Network Device.

**CAUTION**

**Before plugging a cable to any port, be sure to discharge the voltage stored on the cable by touching the electrical contacts to ground surface.**

# Managing Routers and Modules

> **NOTE**
> Wait at least 10 seconds before issuing the **power-off** command and the **power-on** command.

# Maintenance and Field Replacement

> **NOTE**
> Wait at least 10 seconds before issuing the **power-off** command and the **power-on** command.

# Enabling and disabling management module CPU usage calculations

Removed the following note:

> **NOTE**
> When you are finished gathering statistics for debugging purposes, it is recommended that you disable the usage averaging calculations, which are CPU-intensive and can affect the performance of the management module.

# Brocade MLX Series and NetIron XMR supplemental upgrade procedures

## Upgrading MBRIDGE or MBRIDGE32 imageson management modules

> **NOTE**
> Always use TELNET on the MLX-32 chassis (instead of SSH). PROM write operations consume substantial CPU cycles, starving other tasks such as SSH. The end result includes timeouts within affected tasks. TELNET does not have similar issues (i.e. hello exchanges) and hence is not impacted.

# Brocade NetIron CES 2000 Series and NetIron CER 2000 Series supplemental upgrade procedures

## Factory Reset Procedure

The following procedure applies to most managed switches and routers.

⚠ **CAUTION**

**Some commands may vary between vendors.**

From a directly attached serial connection:

1. At the opening CLI prompt, save the current configuration to a TFTP server or other remote device.

2. Enter the following command at the Privileged EXEC level prompt, then press Enter. This command erases the factory test configuration if still present.

   ```
   Brocade# erase startup-config
   ```

   **NOTE**
   Do not execute **write memory**.

⚠ **CAUTION**

**Use the erase startup-config command only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally erase the configuration on a configured system, and decide to abort this factory reset procedure, enter the write memory command to save the running configuration to the startup-config file.**

3. Enter the following command at the Privileged EXEC level prompt, then press Enter:

   ```
   Brocade# reload
   ```

   **NOTE**
   The device may throw a warning that the startup-config cannot be found. This warning can be ignored.

   Once the device has finished reloading, it will be reset to "factory" settings.

4. Configure the device.

# Documentation Updates for the Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide

## In this chapter

The updates in this chapter are for the *Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide*, publication number 53-1002828-01, published July 2013.

**4** In this chapter