

53-1002805-05
25 April, 2014



Brocade MLX Series and NetIron Family

Documentation Updates

Supporting Multi-Service IronWare R05.6.xx

BROCADE

Copyright © 2014 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, MLX, NetIron, SAN Health, ServerIron, TurboIron, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

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
<i>Brocade MLX Series and NetIron Family Documentation Updates</i>	53-1002805-03	NetIron 05.6.00b Release updates.	24 January, 2014
<i>Brocade MLX Series and NetIron Family Documentation Updates</i>	53-1002805-04	NetIron 05.6.00c Release updates.	22 April, 2014
<i>Brocade MLX Series and NetIron Family Documentation Updates</i>	53-1002805-05	Updated Openflow configuration considerations.	25 April, 2014

Contents

About This Document

In this chapter	vii
How this document is organized	vii
Brocade resources	viii
Getting technical help	viii
Document feedback	viii

Chapter 1

Documentation Updates for the Multi-Service IronWare Configuration Guides

In this chapter	1
Configuring a “null” route	2
ACL deny logging	2
Unsupported features for Brocade NetIron CES and Brocade NetIron CER devices	2
Deployment Scenarios and CLI Configuration	3
Telemetry Solutions	4
Scaling limitations	4
Base-line configuration of telemetry solutions	5
Global level configuration	6
PIM over MCT	8
MCT feature interaction	8
Multicast snooping over MCT	8
Running configuration sequence number display	9
Example of show run	9
Example of show access-list I2 command	9
DVMRP legacy protocol support	9
LAG formation rules	9
IPTV support on Brocade NetIron CES and Brocade CER devices ..	11
Configuring a PBR policy	11
HQoS Feature support	12
HQoS for VPLS traffic overview	12
Feature highlights	12
Configuring HQoS for VPLS traffic	12
Limitations	13
Checking for HQoS for VPLS configurations on ports	14

HQoS for LAG traffic overview	14
Feature highlights	14
Configuring steps	15
Limitations	15
WRED support for HQoS	15
Feature highlights	15
Configuring steps	15
Commands	16
Configuring VPLS endpoint over FDP/CDP interface	17
Configuring VLL endpoint over FDP/CDP enabled interface	18
Transparent forwarding of L2 and L3 protocols on a VLL for CES and CER	19
Modify OSPF standard compliance setting	20
VRRP and VRRP-E	20
Configuring an IPv6 Access Control List	21
Start a log file before an upgrade	21
IPv6 packets on Openflow L23 port	22
Before 5.6.00c	22
From 5.6.00c	22
TM RAS Enhancements	23
TM DRAM CRC error interrupt	23
Descriptive TM error interrupt logging	24
Separate Threshold for CRC logging	25
CLI For SFM and Internal FE	25
Simplified Package Upgrade	27
Brocade NetIron XMR and Brocade MLX Series single-command (full-	
system) upgrade	27
Brocade NetIron CER and Brocade NetIron CES single-command	
(full-system) upgrade	28
LP auto-upgrade	28
SCP “success message”	28
L2 protocol packet handling	29
OpenFlow configuration considerations	29

Chapter 2 Documentation updates for Multi-Service IronWare Diagnostic Guide

Chapter 3 Documentation updates for Unified IP MIB Reference

In this chapter	33
Route map configuration table	33
MAC filters	33
RFC 4444: Management Information Base for	
Intermediate System to Intermediate System (IS-IS)	33
Scalar isisSys objects	33

Rate limit counter index table	34
.....	34
Upgrade MIB Objects	35

Chapter 4

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

In this chapter	37
Switch fabric modules	37
Brocade MLXe Series	37
Brocade MLX Series and Brocade NetIron XMR	38
10Gx24-port interface module	38
MLX 48x1G-T interface module	38

About This Document

In this chapter

- [“How this document is organized”](#) on page vii
- [“Brocade resources”](#) on page viii
- [“Getting technical help”](#) on page viii
- [“Document feedback”](#) on page viii

How this document is organized

This document contains updates to the Multi-Service IronWare R05.6.00a product manuals. These updates include document fixes and changes covering new features. [Table 1](#) below list the most recently released Multi-Service IronWare R05.6.00a product manuals.

TABLE 1 Documentation supporting Multi-Service IronWare R05.6.00a

Publication Title	Fabric OS Release	Publication Date
<i>Multi-Service IronWare Administration Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Multiprotocol Label Switch (MPLS) Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare IP Multicast Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Routing Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Software Defined Networking (SDN) Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Security Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Switching Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare QoS and Traffic Management Configuration Guide</i>	R05.6.00a and later	December 2013
<i>Brocade MLXe Series Hardware Installation Guide</i>	R05.6.00a and later	December 2013
<i>Brocade MLX Series and NetIron XMR Hardware Installation Guide</i>	R05.6.00a and later	December 2013
<i>Brocade NetIron CES Series and NetIron CER Series Hardware Installation Guide</i>	R05.6.00a and later	December 2013
<i>Multi-Service IronWare Software Upgrade Guide</i>	R05.6.00a and later	December 2013
<i>Brocade MLX Series and NetIron XMR Diagnostics Guide</i>	R05.6.00a and later	December 2013
<i>Unified IP MIB Reference</i>	R05.6.00a and later	December 2013
<i>Brocade MLX Series and NetIron XMR YANG Guide</i>	R05.6.00a and later	December 2013

Brocade resources

For the latest documentation, go to <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 Multi-Service IronWare Configuration Guides

In this chapter

The updates in this chapter are for the following *Multi-Service IronWare R05.6.00 Configuration Guides*.

- Multi-Service Ironware Switching Configuration Guide - publication number 53-1003036-03
- Multi-Service Ironware Security Configuration Guide - publication number 53-1003035-03

The following features were added or modified as part of the 5.6.00a release.

- [“Configuring a “null” route”](#) on page 2
- [“ACL deny logging”](#) on page 2
- [“Deployment Scenarios and CLI Configuration”](#) on page 3
- [“Telemetry Solutions”](#) on page 4
- [“PIM over MCT”](#) on page 8
- [“Multicast snooping over MCT”](#) on page 8

The following features were added or modified as part of the 5.6.00b release.

- [“HQoS Feature support”](#) on page 12
- [“HQoS for VPLS traffic overview”](#) on page 12
- [“HQoS for LAG traffic overview”](#) on page 14
- [“WRED support for HQoS”](#) on page 15
- [“Configuring VPLS endpoint over FDP/CDP interface”](#) on page 17
- [“Configuring VLL endpoint over FDP/CDP enabled interface”](#) on page 18
- [“Transparent forwarding of L2 and L3 protocols on a VLL for CES and CER”](#) on page 19

The following features were added or modified as part of the 5.6.00c release.

- [“Modify OSPF standard compliance setting”](#) on page 20
- [“VRRP and VRRP-E”](#) on page 20
- [“Configuring an IPv6 Access Control List”](#) on page 21
- [“Start a log file before an upgrade”](#) on page 21
- [“IPv6 packets on Openflow L23 port”](#) on page 22
- [“TM RAS Enhancements”](#) on page 23
- [“Simplified Package Upgrade”](#) on page 27
- [“LP auto-upgrade”](#) on page 28
- [“SCP “success message””](#) on page 28
- [“L2 protocol packet handling”](#) on page 29

Configuring a “null” route

The following section is an update to the Configuring IP Chapter in the *Multi-Service Ironware Switching Configuration Guide*.

The feature support table is updated for the “Dropping Traffic Sent to the Null0 Interface in Hardware” feature.

TABLE 1 Feature support table

Features supported	Brocade Netron XMR	Brocade MLX series	Brocade Netron CES 2000 Series BASE package	Brocade Netron CES 2000 Series ME_PREM package	Brocade Netron CES 2000 Series L3_PREM package	Brocade Netron CER 2000 Series Base package	Brocade Netron CER 2000 Series Advanced Services package
Dropping Traffic Sent to the Null0 Interface in Hardware	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The following note is added in the “Dropping traffic sent to the null0 interface In hardware” section.

NOTE

The **ip hw-drop-on-def-route** command is not supported on the Brocade Netron CES and Brocade Netron CER devices. You can drop traffic sent to the default IP route address in hardware without the **ip hw-drop-on-def-route** command.

ACL deny logging

The following section is an update to the Configuring an IPv6 Access Control List Chapter in the *Multi-Service Ironware Security Configuration Guide*.

ACL deny logging is supported on the Brocade Netron CES and Brocade Netron CER devices but not in conjunction with **acl accounting**, hence updating this section by removing the bullet point “ACL deny logging is not supported”.

Unsupported features for Brocade Netron CES and Brocade Netron CER devices

The following features are not supported on the Brocade Netron CES and Brocade Netron CER devices:

- The **acl-outbound exclude-switched-traffic** command to exclude switched traffic from outbound ACL filtering is not supported.
- The **acl-frag-conservative** command to change the operation of ACLs on fragmented packets is not supported.
- The **suppress-rpf-drop** command to suppress RPF packet drops for a specific set of packets using inbound ACLs is not supported.
- For all Netron devices, if a port has an IPv4 or IPv6 ACL applied, you must remove the ACL bindings before adding that port to a VLAN that has a VE interface.

Deployment Scenarios and CLI Configuration

The following section is an update to the Provider Backbone Bridging (PBB) Networks for the Brocade NetIron XMR and the Brocade MLX series Chapter in the *Multi-Service Ironware Switching Configuration Guide*.

In the Configuration for CE Devices section, under Configuration for PE Devices, the S-VLAN tag-type is 0x9100 and not 0x900.

Telemetry Solutions

The following section is an update to the Telemetry Solutions Chapter in the *Multi-Service Ironware Administration Guide*.

The update provides information about recommended baseline configuration and scaling limitations for telemetry solutions.

Scaling limitations

- 400 (IPv4 and IPv6 combined) route-map instances per interface.
 - Valid instance is a route-map instance with the permit option and with a valid ACL (ACL is present in configuration).
 - Exceeding this limit results in first come first applied behavior on the port.
 - User should redesign their route-map if this limit is exceeded for proper functioning.
- 200 IPv6 ACLs
 - 20480 IPv6 clauses that can be present in the configuration.
- IPv4 ACL limitations have not changed.
- At maximum scale, this configuration may take up to 30 to 45 minutes to bind ACLs used in the route-maps to the ingress interfaces. Traffic is flooded to all VLAN 1 ports during that time.
- User should execute the show cam-partition usage command under the Rule item, to check if it will accommodate the application of the route-map on the desired number of ports on each tower.
- Usage of transparent-hw-flooding (TVF) and transparent-hw-flooding lag-load-balancing (TVF LAG LDB) is best effort, and may result in data loss for bursty streams.
- Usage of per-packet load balancing on LAGs used for TVF LAG LDB is not supported.
- Dynamic and keep-alive LAGs are not supported with TVF LAG LDB.
- If the SFMs are operating in “normal mode”, the number of TVF LAG LDB instances must not exceed the following values. Run the **show vlan tvf-lag-lb** command:

TABLE 2 Configured System Max Values

tvf-lag-lb-fid-group	tvf-lag-lb-fid-pool	Do not exceed value
2	512	170
2	1024	341
2	2048	682
4	512	102
4	1024	204
4	2048	409
8	512	56
8	1024	113
8	2048	227
16	512	30
16	1024	60
16	2048	120

Configuration examples

Base-line configuration of telemetry solutions

```
no spanning-tree
no dual-mode-default-vlan
```

NOTES: Default VLAN must have TVF enabled as shown.

```
vlan 1 name DEFAULT-VLAN
no untagged ethe 13/1 to 13/3
transparent-hw-flooding
```

NOTES: Egress VLANs must have the following as shown.

- 1 A port present
- 2 TVF or TVF LAG LDB enabled
- 3 Port must be enabled
- 4 Port must be in the up state

```
vlan 1000 name Outer_1000
tagged ethe 13/1
transparent-hw-flooding
```

```
vlan 1001 name Outer_1001
tagged ethe 13/2
transparent-hw-flooding
```

```
vlan 1002 name Outer_1002
tagged ethe 13/3
transparent-hw-flooding
```

Global level configuration

Configuring System max and cam-partition

```
system-max vlan 4095
system-max virtual-interface 4095
system-max ip-filter-sys 40960
system-max receive-cam 512
system-max ipv4-mcast-cam 512
system-max ipv6-mcast-cam 512
cam-partition profile ipv4-ipv6
```

Disabling LFS at global level

```
no link-fault-signaling
link-fault-signaling ignore-rx
link-fault-signaling ignore-rx device-1
```

NOTE

These commands prevent link-fault-signaling (LFS) from taking the tap ports offline due to LFS on the monitored links

Configuring Ingress tap port

```
interface ethernet 1/1
enable
ip policy route-map Outer_Mall
ipv6 policy route-map Outer_Mall
allow-all-vlan pbr
gig-default neg-off
mac access-group Deny_Any out
```

NOTE

gig-default neg-off is required to be configured only for 1G fiber ports.

Configuring Egress port

```
interface ethernet 13/1
enable
link-fault-signaling
link-fault-signaling ignore-rx

interface ethernet 13/2
enable
link-fault-signaling
link-fault-signaling ignore-rx

interface ethernet 13/3
enable
link-fault-signaling
link-fault-signaling ignore-rx
```

NOTE

LFS must be enabled on Egress 10G ports.

Configuring ACL

```
ipv6 access-list v6_Mall_Outer_1001
permit ipv6 host 667:a6db:39c5:f217:4374:435e:ba5e:d402 any

ipv6 access-list v6_Mall_Outer_1002
permit ipv6 host 849e:958:ed:bcd8:577d:5468:edef:8dfc any

ipv6 access-list v6_Mall_Outer_1000
permit ipv6 host 2f12:4a71:704c:8a1a:7de3:7ef9:43a9:550a any

ipv6 access-list v6_Permit_Any
permit ipv6 any any

ip access-list extended v4_Mall_Outer_1001
permit ip host 95.64.50.180 any

ip access-list extended v4_Mall_Outer_1002
permit ip host 126.126.14.76 any

ip access-list extended v4_Mall_Outer_1000
permit ip host 117.218.157.45 any

ip access-list extended v4_Permit_Any
permit ip any any

mac access-list Deny_Any
deny any any any
```

NOTE

For this application always set the ACL rule as “permit”.

NOTE

The only exception to this rule is, the last route-map instance must be set as CATCH-ALL, to avoid all unmatched traffic going to the CPU for forwarding. The only exception is if you have another routing protocol which picks up the unmatched traffic, and allows the usage of deny statement in the ACLs and no need to set CATCH-ALL. All “denied” and unmatched packets will be passed to the routing protocol for forwarding. Traffic to be dropped is handled at the end of the route-map.

Configuring Route-map

```
route-map Outer_Mall permit 1000
rule-name 1000
match ip address v4_Mall_Outer_1000
match ipv6 address v6_Mall_Outer_1000
set next-hop-flood-vlan 1000
set interface null0
route-map Outer_Mall permit 1001
rule-name 1001
match ip address v4_Mall_Outer_1001
match ipv6 address v6_Mall_Outer_1001
set next-hop-flood-vlan 1001
set interface null0
route-map Outer_Mall permit 1002
rule-name 1002
match ip address v4_Mall_Outer_1002
match ipv6 address v6_Mall_Outer_1002
set next-hop-flood-vlan 1002
set interface null0
```

```

route-map Outer_Mall permit 10000
rule-name Catch_All
match ip address v4_Permit_Any
match ipv6 address v6_Permit_Any
set interface null0

end

```

Configuration consideration for Route-map

Route-map instances (The complete **route-map blah permit|deny xxx** configuration section) and route-map configuration must meet the following conditions:

1. The last set of commands must be interface null0, this can be preceded by multiple set of other commands. This prevents the matched traffic from going to the CPU for forwarding, when the egress VLAN is not a valid next hop.
2. Rule names can only be used once per route-map.
3. The last route-map instance must be set as CATCH-ALL, to avoid all unmatched traffic going to the CPU for forwarding. The only exception is if you have another routing protocol which picks up the unmatched traffic, and allows the usage of deny statement in the ACLs and no need to set CATCH-ALL. All denied and unmatched packets will be passed to the routing protocol for forwarding.

PIM over MCT

The MCT feature interaction matrix has been updated to indicate that BFD is not supported in NetIron 5.4.00 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.

Running configuration sequence number display

The sequence number display on running configuration has been updated to display as the following example.

Example of show run

```
stub-cat-201(config-mac-acl-in-sample)#show run

sequence 10 permit 0000.0291.1502 ffff.ffff.ffff any 545 etype any
sequence 20 permit 0000.2222.2222 ffff.ffff.ffff any 1201 etype any <-Newly added
ACL rule with sequence number
sequence 30 permit 0000.0201.1502 ffff.ffff.ffff any 401 etype any
```

Example of show access-list l2 command

```
stub-cat-201(config-mac-acl-in-sample)#show access-list l2 in-sample

L2 MAC Access List in-sample : 3 entries
sequence 10 permit 0000.0291.1502 ffff.ffff.ffff any 545 etype any
sequence 20 permit 0000.2222.2222 ffff.ffff.ffff any 1201 etype any <-Newly added
ACL rule with sequence number
sequence 30 permit 0000.0201.1502 ffff.ffff.ffff any 401 etype any
```

DVMRP legacy protocol support

Multi-Service IronWare does not support DVMRP. Use PIM as an alternative protocol for multicast.

LAG formation rules

The LAG formation rules listed below must be followed.

- You cannot configure a port concurrently as a member of a static, dynamic, or keep-alive LAG.
- Any number or combination of ports between 1 and 32 within the same chassis can be used to configure a LAG. The maximum number of LAG ports is checked when adding ports to a LAG.
- All ports configured in a LAG must be of equal bandwidth. For example all 10 G ports.
- All ports configured in a LAG must be configured with the same port attributes.
- LAG formation rules are checked when a static or dynamic LAG is deployed.
- A LAG must have its primary port selected before it can be deployed.
- All ports configured in a LAG must be configured in the same VLAN.

LAG formation rules

- All ports must have the same PBR configuration before deployment. During deployment, the configuration on the primary port is replicated to all ports. On undeployment, each port inherits the same PBR configuration.
- All static LAG ports must have the same LACP BPDU forwarding configuration.
- A LAG member and an individual port cannot use the same name.
- VLAN and inner-VLAN translation

The LAG is rejected if any LAG port has VLAN or inner-VLAN translation configured
- Layer 2 requirements:

The LAG is rejected if the LAG ports:

 - Do not have the same untagged VLAN component.
 - Do not share the same SuperSpan customer ID (CID).
 - Do not share the same VLAN membership or do not share the same uplink VLAN membership
 - Do not share the same protocol-VLAN configuration
 - Are configured as mainly primary and secondary interfaces
 - Static LAG deployment will fail if the if LACP BPDU forwarding is disabled on the primary port and enabled on one or more of the secondary ports.
- Layer 3 requirements:

The LAG is rejected if any of the secondary LAG port has any Layer 3 configurations, such as IPv4 or IPv6 address, OSPF, RIP, RIPNG, IS-IS, and so on.
- Layer 4 (ACL) requirements:
 - All LAG ports must have the same ACL configurations; otherwise, the LAG is rejected.
 - A LAG cannot be deployed if any of the member ports has ACL-based mirroring configured on it.
 - A port with ACL-based mirroring configured on it cannot be added to a LAG.
- The router can support up to 256 LAGs, and each LAG can contain up to 64 member ports.
 - If the router is configured to support 32 LAGs by using the **system-max trunk-num** command, the maximum number of LAG ports is 64.
 - If the router is configured to support 64 LAGs by using the **system-max trunk-num** command, the maximum number of LAG ports is 32.
 - If the **system-max trunk-num** is set to 256, the maximum number of LAG ports supported is 8.
 - The default **system-max trunk-num** is set to 128, and each LAG can have up to 16 member ports
 - For 100G ports, the configurable ranges are from 2 to 16 100G LAGs.
- When configuring a static or dynamic LAG, if trunk load sharing type is set to “per-packet” the maximum number of “per-packet” trunks is set to 4.
- Ports can be in only one LAG group. All the ports in a LAG group must be connected to the same device at the other end. For example, if port 1/4 and 1/5 in Device 1 are in the same LAG group, both ports must be connected to ports in Device 2 or in Device 3. You cannot have one port connected to Device 2 and another port connected to Device 3.
- All LAG member properties must match the primary port of the LAG with respect to the following parameters:

- Port tag type (untagged or tagged port)
- Port speed and duplex
- TOS-based Configuration – All ports in the LAG must have the same TOS-based QoS configuration before LAG deployment, During deployment the configuration on the primary port is replicated to all ports and on undeployment, each port inherits the same TOS-based QoS configuration.

To change port parameters, you must change them on the primary port. The software automatically applies the changes to the other ports in the LAG.

- Using the **system-max trunk-num** *num* *c* command, the device can support the following LAG/member port configurations:
 - 256 LAGs with each containing 8 member ports.
 - 128 LAGs with each containing 16 member ports.
 - 64 LAGs with each containing 32 member ports.
 - 32 LAGs with each containing 64 member ports.

You can change the number of LAGs and member ports by. The valid values are 32, 64, 128, and 256. By default, the router

- Using the **system-max trunk-num-100g** command, the device can support the following 100GbE LAG scalability configurations:
 - 16 LAGs with each containing 2 member ports.
 - 8 LAGs with each containing 4 member ports.
 - 4 LAGs with each containing 8 member ports.
 - 2 LAGs with each containing 16 member ports.

You can change the number of LAGs and member ports by. The valid values are 32, 64, 128, and 256. By default, the router

- The total number of ports in a trunk is controlled by the system-max trunk-num command for both non-100G and 100G trunks.

Make sure the device on the other end of the LAG link can support the same number of ports in the link.

IPTV support on Brocade NetIron CES and Brocade CER devices

Internet Protocol Television (IPTV) multicast streams are supported on Brocade NetIron CES and Brocade NetIron CER devices.

Configuring a PBR policy

NOTE

The following information updates the Configuring a PBR policy section in the Policy-Based Routing chapter.

The “match” and “set” statements described in this section are not supported at the interface level.

HQoS Feature support

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

TABLE 3 Supported platforms

Features supported	Brocade Netron XMR Series	Brocade MLX Series	Brocade Netron CES 2000 Series BASE package	Brocade Netron CES 2000 Series ME_PREM package	Brocade Netron CES 2000 Series L3_PREM package	Brocade Netron CER 2000 Series Base package	Brocade Netron 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 1 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 1 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 successful 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 successful 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
```

WRED support for HQoS

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 **show run** command will display the running configuration information as shown below.

The following examples explain 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.

Transparent forwarding of L2 and L3 protocols on a VLL for CES and CER

Use the `forward-all-protocol` command to add per port Layer 2 and Layer 3 (L2/L3) protocols ACL filters for the VLL end-point port. The command `no forward-all-protocol` removes the L2/L3 protocols ACL filters for the VLL end point port.

NOTE

The `forward-all-protocol` command is only applicable to the Brocade NetIron CER and Brocade NetIron CES.

To implement per port Layer 2 and Layer 3 (L2/L3) protocols ACL filters, enter the following command.

```
Brocade(config)# int eth 1/1
Brocade (config-if-e1000-1/1)# forward-all-protocol
```

Syntax: [no] forward-all-protocol

The command `no forward-all-protocol` deletes VLL end point port L2/L3 protocols ACL filters. For LAG, only the primary port needs to be configured.

NOTE

The `forward-all-protocol` command lets L2/L3 protocols on the port go with hardware forwarding without going to the CPU. If the `no forward-all-protocol` command is executed, the L2/L3 functions may be impacted.

The `show interfaces ethernet slot/port` command displays the configuration status of the `forward-all-protocol` command.

The following output example shows the `show interfaces ethernet slot/port` command with the `forward-all-protocol` command disabled.

```
Brocade# show interfaces ethernet 1/1
GigabitEthernet1/1 is up, line protocol is up
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is GigabitEthernet, address is 001b.eda3.f841 (bia 001b.eda3.f841)
  Configured speed auto, actual 1Gbit, configured duplex fdx, actual fdx
  Member of 1 L2 VLAN(S) (tagged), port is in tagged mode, port state is
Forwarding
  STP configured to ON, Priority is level0, flow control enabled
  Priority force disabled, Drop precedence level 0, Drop precedence force
disabled
  dhcp-snooping-trust configured to OFF
  mirror disabled, monitor disabled
  LACP BPDU Forwarding:Disabled
  LLDP BPDU Forwarding:Disabled
  L2L3 protocols Forwarding:Disabled
  Not member of any active trunks
```

The following output example shows the `show interfaces ethernet slot/port` command with the `forward-all-protocol` command enabled.

```
Brocade(config-if-e1000-1/1)# forward-all-protocol
Brocade(config-if-e1000-1/1)# show interfaces ethernet 1/1
GigabitEthernet1/1 is up, line protocol is up
  STP Root Guard is disabled, STP BPDU Guard is disabled
```

1

Modify OSPF standard compliance setting

```

Hardware is GigabitEthernet, address is 001b.eda3.f841 (bia 001b.eda3.f841)
Configured speed auto, actual 1Gbit, configured duplex fdx, actual fdx
Member of 1 L2 VLAN(S) (tagged), port is in tagged mode, port state is
Forwarding
STP configured to ON, Priority is level0, flow control enabled
Priority force disabled, Drop precedence level 0, Drop precedence force
disabled
dhcp-snooping-trust configured to OFF
mirror disabled, monitor disabled
LACP BPDU Forwarding:Disabled
LLDP BPDU Forwarding:Disabled
L2L3 protocols Forwarding:Enabled
Not member of any active trunks

```

The **forward-all-protocol** command forwards the following protocols by hardware instead of the CPU.

For L2: UDLD (drop), FDP, CDP and MRP.

For L3: IP broadcast (255.255.255.255), IP multicast ((224.0.0.x, 224.0.1.x) including RIP, OSPF, PIM, VRRP), ARP, DHCP, BOOTP, IS-IS, OSPF, ND6, RIPng, OSPFv3, PIMv6, anycast solicited node, DHCPv6.

This command cannot be used on an MPLS interface as it will break existing neighbor relationship.

Modify OSPF standard compliance setting

The following note is added to the “Configuring OSPF Version 2” chapter of the Multi-Service IronWare Routing Configuration Guide under the “Modify OSPF standard compliance setting” section.

NOTE

In the current implementation, the Netron devices are not compliant with RFC3509.

VRRP and VRRP-E

The feature support table for VRRP and VRRP-E chapter is updated with the following changes.

VRRP v3 for IPv4,IPv6 and VRRP-E v6,VRRP alongside OSPF and VRRP alongside BGP4 features are not supported across the Brocade Netron CES 2000 Series BASE package.

TABLE 4

Features supported	Brocade Netron XMR Series	Brocade MLX Series	Brocade Netron CES 2000 Series BASE package	Brocade Netron CES 2000 Series ME_PREM package	Brocade Netron CES 2000 Series L3_PREM package	Brocade Netron CER 2000 Series BASE package	Brocade Netron CER 2000 Series Advanced Services package
VRRP v3 for IPv4 and IPv6	Yes	Yes	No	Yes	Yes	Yes	Yes
VRRP-E v6	Yes	Yes	No	Yes	Yes	Yes	Yes
VRRP alongside OSPF	Yes	Yes	No	Yes	Yes	Yes	Yes
VRRP alongside BGP4	Yes	Yes	No	Yes	Yes	Yes	Yes

Configuring an IPv6 Access Control List

The feature support table for Configuring an IPv6 Access Control List chapter is updated with the following changes.

Filtering IPv6 Packets Based on DSCP Values, Filtering IPv6 Packets Based on Routing Header Type, Applying an IPv6 ACL to a Router Interface, Adding a Comment to an IPv6 ACL Entry, IPv6 Extended ACLs features are not supported across Brocade NetIron CES 2000 Series BASE package.

TABLE 5 IPv6 Access Control List 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
Filtering IPv6 Packets Based on DSCP Values	Yes	Yes	No	Yes	Yes	Yes	Yes
Filtering IPv6 Packets Based on Routing Header Type	Yes	Yes	No	Yes	Yes	Yes	Yes
Applying an IPv6 ACL to a Router Interface	Yes	Yes	No	Yes	Yes	Yes	Yes
Adding a Comment to an IPv6 ACL Entry	Yes	Yes	No	Yes	Yes	Yes	Yes
IPv6 Extended ACLs	Yes	Yes	No	Yes	Yes	Yes	Yes

Start a log file before an upgrade

NOTE

The following recommendation has been added to the Upgrade guide.

It is recommended to start a log file to capture the upgrade process for troubleshooting purposes if an unexpected event occurs.

IPv6 packets on Openflow L23 port

Before 5.6.00c

When a port is configured in Openflow L23 mode (or L23 hybrid mode), IPv6 traffic coming in to that port was processed for traditional IPv6 forwarding (or dropped if the IPv6 routing table does not contain a matching entry).

This behavior was the same for IPv6 traffic even if Openflow flow existed with matching L2 fields. Non-IPv6 traffic was forwarding as per Openflow flow based on L2 match.

From 5.6.00c

If Openflow flow exists with matching L2 fields on an Openflow L23 (hybrid) port, all traffic (including IPv6) matching the L2 fields will be forwarded as per flow.

System-max configuration for Openflow

A new condition has been introduced while configuring system-max for Openflow. The **system-max np-openflow-flow-entries layer2or3** command should be greater than or equal to the **system-max np-openflow-flow-entries layer23ipv4** command.

Hardware entries usage

If Openflow flow exists with matching L2 fields on an Openflow L23 (hybrid) port, it will consume hardware entries from the **system-max np-openflow-flow-entries layer2or3** command along with the **system-max np-openflow-flow-entries layer23ipv4** command.

Example:

For a specific module, consider that **system-max np-openflow-flow-entries layer2or3** is configured as 30,000 and **system-max np-openflow-flow-entries layer23ipv4** is configured as 20,000. If there are 10,000 L2 matching flows on L23 interface, then the maximum number of L2 flows possible will be $(30,000 - 10,000 =) 20,000$ and the maximum number of L23 flows will be $(20,000 - 10,000 =) 10,000$.

TM RAS Enhancements

TM DRAM CRC error interrupt

The TM ingress DRAM CRC needs to be monitored for all line cards and action may need to be taken based on the configuration. The default action is to disable all ports of that TM and this can be overridden by line card reset action through configuration.

```
Brocade(config)#sysmon tm ingress-dram-crc disable
```

Syntax: [no] sysmon tm ingress-dram-crc *action*

disable-ports - ports disable for dram crc errors

none - No action

reset-linecard - linecard reset for dram crc errors

Examples

For default action

TM log

```
Mar 4 20:33:57: Slot 1 PPCR 1 TM Reg offset 0x0000800 Value 0x00000600
```

Syslog

```
Mar 4 20:33:57:A:System: LP15/TM0: All ports down due to Ingress DRAM CRC
Mar 4 20:33:57:I:System: Interface ethernet 15/4, state down - ingress DRAM CRC
Mar 4 20:33:57:I:System: Interface ethernet 15/3, state down - ingress DRAM CRC
Mar 4 20:33:57:I:System: Interface ethernet 15/2, state down - ingress DRAM CRC
Mar 4 20:33:57:I:System: Interface ethernet 15/1, state down - ingress DRAM CRC
```

For line card reset action:

TM log

```
Mar 4 20:33:57: Slot 1 PPCR 1 TM Reg offset 0x0000800 Value 0x00000600
```

Syslog

```
Mar 4 20:33:57: D:System: Module reset in slot 1, triggered by TM Health
Monitoring
Mar 4 20:33:57: D:System: TM Health Monitoring detects an issue in slot 1 ppcr 1
Reg Offset 0x00000800 Value 0x00000040
```

Descriptive TM error interrupt logging

TM Log Messages

Gen1 line cards:

```
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002980 Value 0x00000600 Ingress
(MMU) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002981 Value 0x00000600 Ingress
(MMU) CRC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002080 Value 0x00000600 Ingress
(QDP) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001f80 Value 0x00000600 Ingress
(LBP) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001580 Value 0x00000600 Egress
(EGQ) Reassembly
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002780 Value 0x00000600 Scheduler
(SCH) Flow control
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001a80 Value 0x00000600 Ingress
(INQ) Interrupt
```

Gen2 line cards:

```
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002800 Value 0x00000600 Ingress
(IDR) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002801 Value 0x00000600 Ingress
(IDR) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002a00 Value 0x00000600 Ingress
(IRR) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000400 Value 0x00000600 Ingress
(IQM) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000401 Value 0x00000600 Ingress
(IQM) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000200 Value 0x00000600 Ingress
(IPS) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000800 Value 0x00000600 Ingress
(IPT) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000a00 Value 0x00000600 Ingress
(MMU) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0000a01 Value 0x00000600 Ingress
(MMU) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002e00 Value 0x00000600 Egress
(FDR) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00003800 Value 0x00000600 Egress
(EGQ) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00003801 Value 0x00000600 Egress
(EGQ) Reassembly
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00003803 Value 0x00000600 Egress
(EGQ) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0003a02 Value 0x00000600 Egress
(EPNI) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00004200 Value 0x00000600 Scheduler
(SCH) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001840 Value 0x00000600 Ingress
(DRC) BIST
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001a40 Value 0x00000600 Ingress
(DRC) BIST
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001c40 Value 0x00000600 Ingress
(DRC) BIST
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00001e40 Value 0x00000600 Ingress
(DRC) BIST
```



```

Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002040 Value 0x00000600 Ingress
(DRC) BIST
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002240 Value 0x00000600 Ingress
(DRC) BIST
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00004a00 Value 0x00000600 NIF (NBI)
Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0005800 Value 0x00000600 Egress
(EGQ) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0005802 Value 0x00000600 Egress
(EGQ) Reassembly
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002c00 Value 0x00000600 Ingress
(FDT) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x0005804 Value 0x00000600 Egress
(EGQ) ECC
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002800 Value 0x00000600 Ingress
(IDR) Interrupt
Mar 4 20:33:57: Slot 17 PPCR 2 TM Reg offset 0x00002801 Value 0x00000600 Ingress
(IDR) ECC
    
```

Separate Threshold for CRC logging

```
Brocade(config)#sysmon tm link crc-logging threshold
```

Syntax: `sysmon tm link crc-logging threshold count`

none - No action

sfmlog - sfm/tm logging

syslog - Generate a syslog

Examples

Syslog

```

Mar 4 20:33:57: I:System: Health Monitoring: TM Link CRC errors: SFM5/FE 1/ Link16
-> LP 15/TM 1/link4
    
```

TM log

```
Mar 4 20:33:57: TM Link CRC errors: SNM5/FE1/Link16 ' LP15/TM1/Link4
```

CLI For SFM and Internal FE

```
Brocade(config)#sysmon felink crc-logging threshold
```

Syntax: `sysmon fe link crc-logging threshold action`

none - No action

sfmlog - sfm/tm logging

syslog - Generate a syslog

Example**Syslog**

```
Mar 4 20:33:57: I:System: Health Monitoring: Fabric Link CRC errors:  
LP15/TM1/Link4 ' SNM5/FE1/Link16
```

For Internal FE linecards such as 2x100G and 24x10G

```
Mar 4 20:33:57: I:System: Health Monitoring: Fabric Link CRC errors:  
LP15/FE1/Link4 ' SNM5/FE1/Link16
```

SFM log

```
Mar 4 20:33:57: Fabric Link CRC errors: LP15/TM1/Link4 ' SNM5/FE1/Link16  
Mar 4 20:33:57: Fabric Link CRC errors: LP15/FE1/Link4 ' SNM5/FE1/Link16
```

Simplified Package Upgrade

Simplified Upgrade is a single operation that performs a full system upgrade of all the images. It can be as simple as one command from the CLI or one set-request operation from the SNMP. LP Auto-upgrade allows the system to automatically upgrade the Boot and FPGA images of an inserted interface module.

NOTE

This is not applicable to Brocade NetIron CES and Brocade NetIron CER devices.

The system will always enable FPGA Mismatch-check regardless of whether Auto-upgrade is configured or not. When it finds a mismatch in the FPGA it will put the card to Interactive state with a reason as FPGA-Mismatched.

The LP Auto-upgrade will be modified to start only if the card state is Interactive and the reason is FPGA Mismatched. Since an FPGA mismatch-check has already been done outside the Auto-upgrade, it can proceed to upgrade all the FPGA images applicable to the card.

NOTE

LP Auto-upgrade will only upgrade the FPGA images.

NOTE

LP auto-upgrade is not supported in FIPS mode.

When downgrading from SHA256 signed packages to SHA1 signed packages the following errors might be seen:

```
TFTP: Download to flash done.
TFTP: Download to flash failed - Server Message: File not found
Failed to rename manifest_tmp.sig into manifest.sig
```

NOTE

If this is a downgrade to 5.6B or earlier, the above errors may be ignored.

Brocade NetIron XMR and Brocade MLX Series single-command (full-system) upgrade

There is no change in the syntax for the full-system upgrade; however, the expected behavior for the keyword “all-images” has changed.

Syntax: copy tftp system [all-images] <server-ip-address> manifest <File name> [lp-sec | mp-sec | secondary]

Syntax: copy <slot1 | slot2> system [all-images] manifest <File name> [lp-sec | mp-sec | secondary]

NOTE

BOOT images are not included in the upgrade process. The optional keyword “all-images” specifies to include only the MP FPGA images (MBRIDGE/MBRIDGE32 and SBRIDGE/HSBRIDGE).

Brocade NetIron CER and Brocade NetIron CES single-command (full-system) upgrade

NOTE

BOOT images are not included in the upgrade process. The optional keyword “all-images” specifies to include only the MP FPGA images (MBRIDGE/MBRIDGE32 and SBRIDGE/HSBRIDGE).

Syntax: copy tftp system [all-images] <server-ip-address> manifest <File name> [secondary]

LP auto-upgrade

LP Auto-upgrade does a manifest file integrity check with signatures.

NOTE

LP auto-upgrade is not supported in FIPS mode.

File integrity checks rely on the correct signatures being present on the system at the time of the check, based on the currently running version of the device.

Refer to the **Federal Information Processing Standards and Common Criteria Guide for NetIron 5.6.00** for more information when upgrading from non-SHA256 signatures to SHA256 signature packages or downgrading from SHA256 signature to non-SHA256 signature packages.

When downgrading from SHA256 signed packages to SHA1 signed packages following errors might be seen:

```
TFTP: Download to flash done.  
TFTP: Download to flash failed - Server Message: File not found  
Failed to rename manifest_tmp.sig into manifest.sig
```

NOTE

If this is a downgrade to 5.6B or earlier, the above errors may be ignored.

SCP “success message”

The following update goes in “Configuring Secure Shell and Secure Copy” chapter, under “Using Secure Copy” section.

NOTE

The **scp** command will not display any “success message” on completion of data transfer. Instead use **showlog** command to validate scp image success.

L2 protocol packet handling

The following content has been modified in the Multi-Chassis Trunking (MCT) chapter in the "L2 protocol packet handling" section.

If the **no cluster-l2protocol-forward** command is configured on global basis or **cluster-l2protocol-forward disable** is configured on a port, the STP protocol packets coming on the ICL ports of MCT VLANs are dropped.

All other L2 protocol packets will be flooded on the MCT VLANs or dropped. The **cluster-l2protocol-forward** command is not applicable to these protocol packets. It only applies to STP or RSTP BPDU packets on the ICL ports only.

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:

- OpenFlow action can duplicate traffic to 16 ports.
- It supports Administratively down (OFPPC_PORT_DOWN) through Port Modification Message.

Documentation updates for Multi-Service IronWare Diagnostic Guide

NOTE

There are no updates for NetIron 5.6.00b.

NOTE

There are no updates for NetIron 5.6.00c.

Documentation updates for Unified IP MIB Reference

In this chapter

The updates in this chapter are for the *Unified IP MIB Reference*, published December 2013.

Route map configuration table

Name, OID, and syntax	Access	Description
brcdRouteMapRuleName brcdIp.1.1.3.39.1.1.1.1.4 Syntax: DisplayString NOTE: This object is not supported on the Brocade NetIron CES and Brocade NetIron CER series devices.	Read-create	Identifies the path name for the route map. A maximum of 127 characters is allowed.

MAC filters

NOTE
MAC filter MIB objects are not supported on the Brocade NetIron XMR, Brocade MLX series, Brocade NetIron CES, and Brocade NetIron CER series devices.

RFC 4444: Management Information Base for Intermediate System to Intermediate System (IS-IS)

Scalar isisSys objects

Object group name	Object identifier	Supported?	Notes
isisSysMaxPathSplits	1.3.6.1.2.1.138.1.1.1.4	Yes	Default value is 4 on the Brocade NetIron devices.

Rate limit counter index table

The following table objects map each row indexes of rate limit counter table entries to their corresponding ACL or VLAN or VLAN Group ID.

Name, OID, and syntax	Access	Description
agRateLimitCounterIndexTable brcdIp.1.1.3.16.1.3	None	The rate limit counter index table.
agRateLimitCounterIndexRowIndex brcdIp.1.1.3.16.1.3.1.1 Syntax: Integer	Read-only	The table index for rate limit objects. It increases as the rate limit entries are added and skips the number when a row is deleted. Valid values: 1– 2147483647
agRateLimitCounterIndexDirection brcdIp.1.1.3.16.1.3.1.2 Syntax: PacketSource	Read-only	The input or output transmission direction for the rate limit object. <ul style="list-style-type: none"> input (0) – For inbound traffic output(1) – For outbound traffic
agRateLimitCounterIndexACLID brcdIp.1.1.3.16.1.3.1.3 Syntax: Integer32	Read-only	The corresponding ACL ID to match the row index of the rate limit counter table.
agRateLimitCounterIndexVLANID brcdIp.1.1.3.16.1.3.1.4 Syntax: Integer32	Read-only	The corresponding VLAN ID to match the row index of the rate limit counter table.
agRateLimitCounterIndexVLANGroupID brcdIp.1.1.3.16.1.3.1.5 Syntax: Integer32	Read-only	The corresponding VLAN Group ID to match the row index of the rate limit counter table.
agRateLimitCounterIndexMACAddress brcdIp.1.1.3.16.1.3.1.6 Syntax: MAC address	Read-only	The corresponding MAC Address for Source MAC-based rate limit to match the row index of the rate limit counter table.

Upgrade MIB Objects

The description of the following two MIB objects has been updated for the Multi-Service IronWare Release 05.6.00c.

Name, OID, and syntax	Access	Description
brcdSwPackageUpgradeAllImages brcdIp.1.1.2.16.1.1.4 Syntax: TruthVal	Read-write	<p>Specifies all images upgrade.</p> <ul style="list-style-type: none"> true(1) - The upgrade sequence includes MP FPGA images (MBRIDGE/MBRIDGE32 and SBRIDGE/HSBRIDGE). false(2) - Upgrades only MP and LP monitor images, MP and LP application images, and LP bundled FPGA images for the Brocade Netron XMR and the Brocade MLX Series. For Brocade Netron CES and Brocade Netron CER series, only the monitor, application, and FPGA images are upgraded. Returns false(2), for a read-only operation. <p>Default: false(2)</p>
brcdSwIntfModAutoUpgradeAllImages brcdIp.1.1.2.16.1.2.5 Syntax: TruthValue	Read-write	<p>Specifies all images upgrade.</p> <ul style="list-style-type: none"> The upgrade sequence includes only the LP boot image, if set to true(1). The default false(2), upgrades only the LP FPGA images. <p>Returns false(2), for a read-only operation.</p> <p>NOTE: This object is deprecated. SET operation is not supported and READ operation will return false(2).</p>

Upgrade MIB Objects

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

In this chapter

The updates in this chapter are for the following publications:

- Brocade MLXe Series Hardware installation Guide - publication number 53-1003030-02
- Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide - publication number 53-1003040-02

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. 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 (4-, 8-, and 16-slot routers only)	The switch fabric is on (active) and ready to switch user packets.
		On (32-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. 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.

10Gx24-port interface module

For maximum performance, you will need to change the **system-init tm-credit-size** to **credit_1024b**. Log into your system and enter the following commands in the configuration level of the CLI. It is important to issue commands to **write memory** and **reload** the device.

```
Brocade# config
Brocade(config)# system-init tm-credit-size credit_1024b
Brocade(config)# exit
Brocade# write memory
Brocade# reload
```

MLX 48x1G-T interface module

In prior releases the MLX 48x1G-T module was listed as GEN1 module. As of NetIron 5.6.00c the MLX 48x1G-T module is listed as a GEN1.1 module.