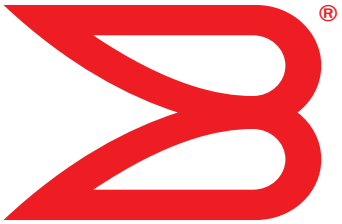
53-1003301-10
4 February 2015



Brocade MLX Series and NetIron Family

Documentation Updates

Supporting Multi-Service IronWare R05.6.xx

BROCADE

Copyright © 2015 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

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 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

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
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-03	NetIron 05.6.00b Release updates.	24 January, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-04	NetIron 05.6.00c Release updates.	22 April, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-05	Updated Openflow configuration considerations.	25 April, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-06	NetIron 05.6.00d Release updates.	31 July, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-07	NetIron 05.6.00d Release updates version 2.	8 August, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-08	NetIron 05.6.00d Release updates in Chapter 4.	21 August, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-09	NetIron 05.6.00e Release updates	16 December, 2014
Brocade MLX Series and NetIron Family Documentation Updates	53-1003301-10	NetIron 05.6.00f Release updates	4 February, 2015

Contents

About This Document

In this chapter ix
How this document is organized ix
Brocade resources x
Getting technical help x
Document feedback x

Chapter 1 Documentation Updates for the Multi-Service IronWare Configuration Guides

In this chapter 1
Configuring a “null” route 3
ACL deny logging 3
Unsupported features for Brocade NetIron CES and Brocade NetIron CER devices 3
Deployment Scenarios and CLI Configuration 4
Telemetry Solutions 5
Scaling limitations 5
Base-line configuration of telemetry solutions 6
Global level configuration 7
PIM over MCT 9
MCT feature interaction 9
Multicast snooping over MCT 9
Running configuration sequence number display 10
Example of show run 10
Example of show access-list l2 command 10
DVMRP legacy protocol support 10
LAG formation rules 10
IPTV support on Brocade NetIron CES and Brocade CER devices . . 12
Configuring a PBR policy 12
HQoS Feature support 13
HQoS for VPLS traffic overview 13
Feature highlights 13
Configuring HQoS for VPLS traffic 13
Limitations 14
Checking for HQoS for VPLS configurations on ports 15

HQoS for LAG traffic overview 15
Feature highlights 15
Configuring steps 16
Limitations 16
WRED support for HQoS 16
Feature highlights 16
Configuring steps 16
Commands 17
Configuring VPLS endpoint over FDP/CDP interface 18
Configuring VLL endpoint over FDP/CDP enabled interface 19
Transparent forwarding of L2 and L3 protocols on a VLL for CES and CER 20
Modify OSPF standard compliance setting 21
VRRP and VRRP-E 21
Configuring an IPv6 Access Control List 22
Start a log file before an upgrade 23
IPv6 packets on Openflow L23 port. 24
Before 5.6.00c 24
From 5.6.00c 24
TM RAS Enhancements 25
TM DRAM CRC error interrupt 25
Descriptive TM error interrupt logging 26
Separate Threshold for CRC logging. 28
Simplified Package Upgrade 29
Brocade NetIron XMR and Brocade MLX Series single-command (full-system) upgrade 29
Brocade NetIron CER and Brocade NetIron CES single-command (full-system) upgrade 30
LP auto-upgrade 30
SCP “success message” 30
L2 protocol packet handling. 31
OpenFlow configuration considerations 31
Configuring egress buffer threshold 32
TM XPP link status check 33
Flow control handling modification 34
CLI commands 34
Policy-based routing support for preserve VLAN. 34
Deletion of ACLs bound to an interface. 35
Optional cluster operation features 36
Enabling a transparent firewall 36
Default VRRP/VRRP-E dead interval calculation 37
IPv6 anycast filtering. 37

PBIFS extended counters 38
Limiting log generation for MEP and Remote MEP 38
IPv4 ACL-based rate limiting updates 39
Configuration considerations 39
Configuring a port-and-ACL-based traffic policing policy 39
How the Brocade device processes ACLs 39
FE access recovery disable 40
Usage Guidelines 40
Output 40
Setting the delay before bringing up the CCEP port 41
Setting the OpenFlow system maximum 41
IPv6 Multicast Listener Discovery snooping 42
Configuring IPv6 multicast routing or snooping 42
Enabling IPv6 multicast traffic reduction 42
Configuring and enabling sFlow 43
Multicast queue size, flow control, rate shaping and egress buffer threshold 43
Enabling PVST+ support 44
Assigning or changing a VLAN priority 44
Specifying the number of MAC addresses to be denied 44
Specifying the number of MAC addresses to be denied 44
NTP loss of sync message 45
Path selection metric for CSPF computation 45
Path selection for CSPF computation 45
Configuring TE-metric for MPLS interface 46
Configuring the CSPF computation mode 47
Configuring TE-metric for an interface 47
Configuring the CSPF computation mode value at global level 47
Configuring the CSPF computation mode value for primary LSPs 48
Configuring the CSPF computation mode value for secondary LSPs 48
Configuring the CSPF computation mode value for static bypass LSPs 48
Configuring the CSPF computation mode value for dynamic bypass LSPs 49
No advertising of inter-vrf-leaked routes out to L3VPN 49
AES-CTR encryption mode support for SSH 50
2x100G XPP ILKN Monitoring 51
sysmon np interlaken-monitor 51

Chapter 2 Documentation updates for Multi-Service IronWare Diagnostic Guide

In this chapter 53
CPU memory show commands 53

Chapter 3 Documentation updates for Unified IP MIB Reference

In this chapter 55
Route map configuration table. 55
MAC filters 55
RFC 4444: Management Information Base for Intermediate System to Intermediate System (IS-IS) 55
Scalar isisSys objects 55
Rate limit counter index table 56
Upgrade MIB Objects 57
Upgraded MIB Objects 58

Chapter 4 Documentation Updates for the MLXe / MLX Series and NetIron XMR Series Hardware Installation Guide

In this chapter 59
Switch fabric modules 59
Brocade MLXe Series. 59
Brocade MLX Series and Brocade NetIron XMR 60
10Gx24-port interface module. 60
MLX 48x1G-T interface module 60
PBIF Recovery 61
Syntax 61
Command Default 61
Examples 61
Router modules. 61
TX drain support 62

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

Chapter 1

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 3
- "ACL deny logging" on page 3
- "Deployment Scenarios and CLI Configuration" on page 4
- "Telemetry Solutions" on page 5
- "PIM over MCT" on page 9
- "Multicast snooping over MCT" on page 9

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

- "HQoS Feature support" on page 13
- "HQoS for VPLS traffic overview" on page 13
- "HQoS for LAG traffic overview" on page 15
- "WRED support for HQoS" on page 16
- "Configuring VPLS endpoint over FDP/CDP interface" on page 18
- "Configuring VLL endpoint over FDP/CDP enabled interface" on page 19
- "Transparent forwarding of L2 and L3 protocols on a VLL for CES and CER" on page 20

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

- "Modify OSPF standard compliance setting" on page 21
- "VRRP and VRRP-E" on page 21
- "Configuring an IPv6 Access Control List" on page 22
- "Start a log file before an upgrade" on page 23
- "IPv6 packets on Openflow L23 port" on page 24
- "TM RAS Enhancements" on page 25
- "Simplified Package Upgrade" on page 29
- "LP auto-upgrade" on page 30
- "SCP "success message"" on page 30
- "L2 protocol packet handling" on page 31

1 In this chapter

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

- "OpenFlow configuration considerations" on page 31
- "Configuring egress buffer threshold" on page 32
- "TM XPP link status check" on page 33
- "Flow control handling modification" on page 34
- "Policy-based routing support for preserve VLAN" on page 34
- "Deletion of ACLs bound to an interface" on page 35
- "Optional cluster operation features" on page 36
- "Enabling a transparent firewall" on page 36
- "Default VRRP/VRRP-E dead interval calculation" on page 37
- "IPv6 anycast filtering" on page 37
- "PBIFS extended counters" on page 38
- "Limiting log generation for MEP and Remote MEP" on page 38
- "IPv4 ACL-based rate limiting updates" on page 39
- "FE access recovery disable" on page 40
- "Setting the delay before bringing up the CCEP port" on page 41
- "Setting the OpenFlow system maximum" on page 41
- "IPv6 Multicast Listener Discovery snooping" on page 42

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

- "Specifying the number of MAC addresses to be denied" on page 44
- "NTP loss of sync message" on page 45
- "Path selection metric for CSPF computation" on page 45
- "No advertising of inter-vrf-leaked routes out to L3VPN" on page 49
- "AES-CTR encryption mode support for SSH" on page 50
- "2x100G XPP ILKN Monitoring" on page 51

NOTE
No features were added or modified as part of the for NetIron 5.6.00f.

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 NetIron XMR	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
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 NetIron CES and Brocade NetIron 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 NetIron CES and Brocade NetIron 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 NetIron CES and Brocade NetIron CER devices

The following features are not supported on the Brocade NetIron CES and Brocade NetIron 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 NetIron 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

Table 0.1:

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 xxxx** 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.

- 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 NetIron 5.5.00. The following documentation supplements the *Multi-Service IronWare QoS and Traffic Management Configuration Guide*.

TABLE 3 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 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
```

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.

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
```

```
    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 NetIron 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 NetIron CES 2000 Series BASE package.

TABLE 4

Table 0.2:

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
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

Table 0.3:

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 *Multi-Service Ironware 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

syslog - syslog will be added 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
```

For syslog action

```
May 18 12:06:04:A:System: LP15/TM0: dram crc errors are detected
```

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*

For action:

syntax - sysmon tm link crc-logging action

none - No action

tmlog - 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 *count*

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

For action:

none - No action

sfmlog - sfm 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.

Configuring egress buffer threshold

NOTE
The following command is available in all versions of NetIron 5.6.00.

The current configuration egress buffer threshold per port is set to 50% of total egress buffer size. Using the followi3ng command you can set the egress buffer threshold up to 95% of total egress buffer size which helps reduce egress packet drops when there is a high amount of traffic.

NOTE
It is recommended to use this command when a sudden burst is seen in traffic and not for general use.

Syntax: Syntax: qos multicast egress-max-buffer port { [guaranteed_max_buffer] [best-effort_max_buffer] }

```
Brocade#config terminal
Brocade(config)#interface ethernet 1/1
Brocade(config-if-e10000-1/1)# qos multicast egress-max-buffer port 95% 90%
```

The **guaranteed_max_buffer** specifies the maximum buffer size allowed per port for guaranteed traffic flow (multicast port priority 3). Specified as percentage of total buffer size.

The **best-effort_max_buffer** specifies the maximum buffer size allowed per port for guaranteed traffic flow (multicast port priority 2-0). Specified as percentage of total buffer size.

Additionally you can also have the threshold configured for individual ports so that each port has its dedicated buffer space.

The example uses a 8x10 line card and has four ports per TM. The buffer size is divided into quarters, so that each port has 1/4 of the total buffer size as its dedicated buffer space.

```
Brocade# config terminal
Brocade(config)# interface ethernet 1/1
Brocade(config-if-e10000-1/1)# qos egress-max-buffer port 24% 23%
```

TM XPP link status check

The link between TM and XPP is periodically monitored to determine link issues at run time and perform appropriate recovery.

```
Brocade(config)#sysmon tm nif-check threshold count 120

Brocade(config)#sysmon tm nif-check disable-ports
```

Syntax: [no] sysmon tm nif-check threshold *count* *polling period*

Syntax: [no] sysmon tm nif-check *action*

disable-ports ports disable for nif errors

reset-linecard linecard reset for nif errors

Examples

Default action:

```
Syslog:Mar 4 20:33:57:A:System: LP15/TM0: All ports down due to TM XPP link
down
Mar 4 20:33:57:I:System: Interface ethernet 15/4, state down - TM XPP link
down
Mar 4 20:33:57:I:System: Interface ethernet 15/3, state down - TM XPP link
down
Mar 4 20:33:57:I:System: Interface ethernet 15/2, state down - TM XPP link
down
Mar 4 20:33:57:I:System: Interface ethernet 15/1, state down - TM XPP link
down
```

Snmp trap:

```
Health Monitoring: LP15: All ports down due to TM XPP link down
```

Line card reset action:

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
TM XPP link down
```

Snmp trap:

```
Type- debugging
System: Module reset in slot 1, triggered by TM Health Monitoring
```

Flow control handling modification

A CLI command has been added to configure the flow control to default settings.

CRC errors were seen on ports connected to 8x10G modules, due modifications to the flow control settings. To avoid these errors, it is recommended to configure the flow control to default settings.

CLI commands

The `tx-drain-disable` command disables the Tx drain on MAC. The no `tx-drain-disable` command enables the Tx drain on MAC. This command can be used on either the global level or interface level.

Global command

```
Brocade(config)#flow-control tx-drain-disable
```
Syntax: [no] flow-control tx-drain-disable

Interface command

```
Brocade(config-if-e10000-16/7)#flow-control tx-drain-disable
```
Syntax: [no] flow-control tx-drain-disable

The `tx-drain-disable` command disables the Tx drain on MAC. The no `tx-drain-disable` command enables the Tx drain on MAC.

Policy-based routing support for preserve VLAN

NOTE
The description in the section “Policy-based routing support for preserve VLAN” has been updated to include the following text.

When the PBR TVF VLAN egress ports are in dual VLAN mode, the ingress tagged packets flood as “tagged” with the original VLAN ID and priority preserved. The ingress untagged packets flood as “untagged” if the egress port is the untagged member of the ingress port's default VLAN; otherwise, the ingress untagged packets flood as “tagged” with the original VLAN ID and priority preserved.

Deletion of ACLs bound to an interface

The following note has been added to the ACL chapter in the above section of the *Multi-Service Ironware Security Configuration Guide*.

To delete an ACL bound to an interface, use the **force-delete-bound-acl** command.

NOTE
This command is also supported on Brocade NetIron CES Series and Brocade NetIron CER Series devices.

To delete an ACL bound to an interface, use the **force-delete-bound-acl** command.

Initially **force-delete-bound-acl** is disabled.

```
Brocade(config)#acl-policy
Brocade(config-acl-policy)# force-delete-bound-acl
```

The **no force-delete-bound-acl** command does not allow the ACLs bound to an interface to be deleted.

```
Brocade(config-acl-policy)# no force-delete-bound-acl
```

Syntax: [no] force-delete-bound-acl

When **force-delete-bound-acl** is enabled, it allows deletion of ACLs bound to one or more interfaces. After enabling this command for the deletion of the ACLs, however the binding of the ACL to an interface still remains. On rebinding this will be an empty ACL and will have no affect on traffic forwarding. On rebinding the CAM entries are reprogrammed appropriately, so no ACL filtering takes place after the ACL is deleted. This command is available as a subcommand of **acl-policy** command. However like any other ACL modification the CAM is only reprogrammed during rebind. Without a rebind the old filters are still present in the CAM.

NOTE
In case of subnet broadcast ACL bindings, when an empty ACL is bound to an interface, implicit deny entries are programmed to the CAM and will have effect on traffic forwarding.

NOTE
This command is also supported on Brocade NetIron CES and Brocade NetIron CER Series devices.

An example of the command is as below.

```
Brocade(config-acl-policy)# force-delete-bound-acl
Brocade(config-acl-policy)# exit
Brocade(config)# show access-list all
ACL configuration:
!
mac access-list SampleACL
permit any any 10 etype any
!
Brocade(config)# show access-list bindings
L4 configuration:
!
interface ethe 2/1
mac access-group SampleACL in
!
Brocade(config)#show cam l2acl
SLOT/PORT Interface number
```

```
Brocade(config)# sh cam l2acl 2/1
LP Index   VLAN Src MAC       Dest MAC     Port  Action  PRAM
    (Hex)                                                Hex)
2 0a3800  10  0000.0000.0000 0000.0000.0000 0   Pass    0009c
2 0a3802  0   0000.0000.0000 0000.0000.0000 0   Drop    0009d
Brocade(config)#
Brocade(config)#no mac acc SampleACL
Brocade(config)#sh cam l2acl 2/1
LP Index VLAN Src MAC Dest MAC Port Action PRAM
(Hex) (Hex)
Brocade(config)#show access-list all ACL configuration:
!
Brocade(config)#show access-list bindings
L4 configuration:
!
interface ethe 2/1 mac access-group SampleACL in
!
Brocade(config)#
```

Optional cluster operation features

The following content has been modified in the Multi-Chassis Trunking (MCT) chapter of the *Multi-Service Ironware Switching Configuration Guide*. The update is part of the “Client interfaces delay” section.

The default value for delay is 90 seconds. The acceptable values range between 20 and 1800 seconds.

Enabling a transparent firewall

The following note has been added to the VLANS chapter of the *Multi-Service Ironware Switching Configuration Guide*. The update is part of the “Transparent firewall mode” section.

NOTE
Transparent firewall mode is available only on the Brocade NetIron CES and Brocade NetIron CER devices.

To set the mode to transparent, enter a command such as the following.

```
Brocade(config-vlan-10)# transparent-fw-mode
```

To set the mode to routed, enter a command such as the following.

```
Brocade (config-vlan-10)# no transparent-fw-mode
```

Syntax: [no] transparent-fw-mode

Transparent firewall mode is available only on the Brocade NetIron CES and Brocade NetIron CER devices

Default VRRP/VRRP-E dead interval calculation

Dead Interval is the number of seconds a Backup waits for a Hello message from the Master before determining that the Master is dead. When Backups determine that the Master is dead, the Backup with the highest priority becomes the new Master. The Dead interval can be set from 1 - 84 seconds. The default is internally derived by software.

- It is equal to 3 times the Hello interval + Skew time
- Where Skew time is equal to (256 - priority) divided by 256.

To change the Dead interval on a Backup to 30 seconds for VRRPv2 and VRRP-Ev2, enter the following commands.

```
Brocade(config)# interface ethernet 1/5
Brocade(config-if-e10000-1/5)# ip vrrp vrid 1
Brocade(config-if-e10000-1/5-vrid-1)# dead-interval 30
```

Syntax: [no] dead-interval *value*

IPv6 anycast filtering

By default all IPv6 packets with anycast address as destination will be processed. The following command provides options to selectively enable protocols or disable all protocols.

```
Brocade(config)# ipv6 anycast-no-response allow tcp
```

Syntax: [no] ipv6 anycast-no-response [allow <tcp|udp|icmp>]

The **allow tcp | udp | icmp** specifies the protocol to allow for processing.

Note:

1. The **allow** options can also be used as standalone commands. If **ipv6 anycast-no-response** is already configured, it is modified based on the specified filters.
2. User can enable generation of TCP resets for incoming TCP packets with destination set as anycast address, by configuring **ip tcp enable-reset** command. However, if **ipv6 anycast-no-response** command is also enabled, this command becomes void since all anycast packets are blocked. If user requires reset to be sent for incoming anycast TCP packets, user has to configure **ipv6 anycast-no-response allow tcp** to unblock the incoming TCP packets.

PBIFS extended counters

The following statistics are maintained by Stats FPGA for each of two XPPs on board

TABLE 6

Counter Type	Number of Counters per XPP (For legacy 8x10G XMR mode)	Number of Counters per XPP (Extended in SW5.7)
FWD/Flow Counter (Packets	512k	512k
FWD/Flow Counter (Bytes)	512k	512k
Port/Vlan/Pri Stats (Packets)	32k	64k
Port/Vlan/Pri Stats (Bytes)	32k	64k
ACL/LSP Stats (Packets)	64k	128k
ACL/LSP Stats (Bytes)	64k	128k
Port/Vlan/Pri Stats (Packets)	32k	32k
Port/Vlan/Pri Stats (Bytes)	32k	32k

Limiting log generation for MEP and Remote MEP

Use the **logs-per-interval-per-mep-rmep** *value* command to limit the number of logs generated for each MEP or RMEP in a 15 minute time window. The following example limits the log generation to 20 logs per MEP or RMEP in a 15 minute time window. The command is enabled under the CFM Protocol Configuration mode.

```
Brocade(config)#cfm-enable
Brocade(config-cfm)#logs-per-interval-per-mep-rmep 20
Brocade(config-cfm)#
```

Syntax: logs-per-interval-per-mep-rmep *value*

The *value* parameter specifies the number of logs generated per MEP or RMEP per 900000 milliseconds. The decimal range is from 1 to 100. The default is 10. When the *value* parameter is configured, the value is uniform for all MEPs and RMEPs. The command is not enabled by default. The **no** form of the command resets the value to the default value of 10.

NOTE
Limiting log generation is supported on Brocade NetIron XMR and Brocade MLX series devices, and Brocade NetIron CES and Brocade NetIron CER devices.

Use the **show cfm logs-limit-per-mep-rmep** command to display the *value* parameter configured for the log limit generation for each MEP or RMEP. The *value* parameter is highlighted in the output.

```
Brocade(config-cfm)#show cfm logs-limit-per-mep-rmep
Logs limit per interval (900000 ms) per MEP/RMEP : 15 (Default : 10)
```

Syntax: show cfm logs-limit-per-mep-rmep

IPv4 ACL-based rate limiting updates

The following updates are made in *Multi-Service Ironware Traffic Management Guide* under **Configuration considerations** and **Configuring a port-and-ACL-based traffic policing policy** sections of the "**Configuring Traffic Policing for the Brocade NetIron CES and Brocade NetIron CER**" chapter.

Configuration considerations

- IPv4 ACL-based rate limiting is not supported on VPLS and VLL endpoints.
- IPv4 ACL-based rate limiting on a port that belongs to a VLAN is not supported on a VLAN without a VE configured.
- IPv4 ACL-based rate limiting is not supported on a port that belongs to a VLAN where in Layer 3 Interface (VE) is configured for MPLS.

Configuring a port-and-ACL-based traffic policing policy

- IPv4 ACL-based rate limiting is not supported on VPLS and VLL endpoints.
- IPv4 ACL-based rate limiting on a port that belongs to a VLAN is not supported on a VLAN without a VE configured.
- IPv4 ACL-based rate limiting is not supported on a port that belongs to a VLAN where in Layer3 Interface (Ve) is configured for MPLS.

How the Brocade device processes ACLs

The following updates are made in the *Multi-Service Ironware Security Guide* under **How the Brocade device processes ACLs**, General configuration guidelines section of the "**Access Control List**" chapter.

General configuration guidelines

- IPv4 ACL-based rate limiting on a port that belongs to a VLAN is not supported on a VLAN without a VE configured.
- IPv4 ACL-based rate limiting is not supported on a port that belongs to a VLAN where in Layer 3 Interface (Ve) is configured for MPLS.

FE access recovery disable

To disable a RAS feature that will power-cycle a switch fabric module if SW cannot access fabric element.

Syntax: system-init fe-access-recovery-disable

Usage Guidelines

The system does the periodic monitoring of FE access and keeps a log for this by code monitoring fabric links and kicks off when number of links down exceeds defined threshold for traffic. However if failure detection configuration is enabled, you need to use these commands for recovery.

Output

The ~ system-init ~ command configures the following information:

TABLE 7

Command	Description
block-g1-sfm	Configure the system to block g1 switch fabric module.
fabric-data-mode	Configure the fabric data mode.
fabric-failure-detection	Configure the system to automatically detect and shutdown failure fabric
fe-access-recovery-disable	Configure fabric element access failure recovery disable.
max-tm-queues	Configure maximum number queues in traffic manager to 4.
mlxe32-24x10g-enable	Configure the system to accept 24x10G module.
tm-credit-size	Configure traffic manager credit size.

Examples:

```
Brocade(config)#system-init fe-access-recovery-disable
Brocade(config)#system-init fe-access-recovery-disable
Brocade(config)#no system-init fe-access-recovery-disable
Brocade(config)#
```

Setting the delay before bringing up the CCEP port

Use the **client-interfaces delay** command to set the delay before bringing up the CCEP port. This command is used to set the delay, so that after a node is reloaded, with just L2vpn peer alone, the delay to bring up the CCEP port will be the designated value.

```
Brocade(config-cluster-TOR)#client-interfaces delay 60
```

Syntax: no] client-interfaces delay *time in sec*

The default value for delay is 90 seconds. The acceptable values range between 20 to 1800 seconds.

Setting the OpenFlow system maximum

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

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

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

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

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

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

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

The *value* variable represents the number of port and unprotected VLAN combination entries that can be configured in the system. The range is from 0 to 4096. after using this command, you must reload the system.

IPv6 Multicast Listener Discovery snooping

IPv6 Multicast Listener Discovery (MLD) snooping controls the amount of multicast traffic in a switched network. By default, a LAN switch floods the broadcast domain with multicast IPv6 packets. If many multicast servers are sending streams to the segment, this will consume a lot of bandwidth. MLD snooping identifies multicast-enabled router ports and multicast receiver ports in a given VLAN or a switched network and forwards multicast traffic only to those ports.

Configuring IPv6 multicast routing or snooping

IPv6 multicast snooping or routing can be enabled on a VE interface or VLAN, but not on both. This is because all of the multicast data and control packets received on the snooping VLAN are handled by multicast snooping and do not reach the multicast routing component. Similarly, any multicast data or control packets received on a VE interface enabled with PIM or Distance Vector Multicast Routing Protocol (DVMRP) routing are handled by the PIM or DVMRP routing component and are not seen by the MLD snooping component.

The following considerations apply when configuring concurrent operation of multicast routing and snooping.

- Either multicast snooping or routing can be enabled on a VE or VLAN but not both.
- Snooping can be enabled globally (ipv6 multicast active | passive).
- The global snooping configuration is inherited by all current VLANs that are not enabled for multicast routing.
- The global snooping configuration is also inherited by all new VLANs. To enable multicast routing on a newly configured VE or VLAN (when snooping is globally enabled), you must first disable snooping on the newly created VE or VLAN.
- Global snooping configuration must be configured first before VLAN configuration.
- A VLAN-level snooping configuration is displayed only if it is different from the global configuration.

NOTE
MLD snooping in a layer 2 switch works properly, when you use a configured VE interface with IPv6 address.

Enabling IPv6 multicast traffic reduction

By default, the device forwards all IPv6 multicast traffic out to all ports except the port on which the traffic was received. To reduce multicast traffic through the device, you can enable IPv6 Multicast Traffic Reduction. This feature configures the device to forward multicast traffic only on the ports attached to multicast group members, instead of forwarding all multicast traffic to all ports. The device determines the ports that are attached to multicast group members based on entries in the MLD Snooping table. Each entry in the table consists of MAC addresses.

Configuring and enabling sFlow

The following note is removed from the Configuring and enabling sFlow section in the sFlow chapter of the *Brocade MultiService IronWare Switching Configuration Guide*.

NOTE
If you change the router ID or other IP address value that sFlow uses for its agent_address, you must disable and then re-enable sFlow to use the new source address.

Multicast queue size, flow control, rate shaping and egress buffer threshold

NOTE
The following section is applicable for the *Multi-Service Ironware Traffic Management Guide* under the section titled Multicast queue size, flow control, rate shaping and egress buffer threshold.

The following commands are only applicable for the Brocade MLX Series platform. These commands are not operable on the Brocade NetIron CER or Brocade NetIron CES platforms.

```
qos multicast-queue-type queue-number max-queue-size queue-size

qos multicast flow-control

qos multicast shaper [guaranteed | best-effort ] rate bandwidth

qos multicast egress-max-buffer port { [guaranteed_max_buffer]
[best-effort_max_buffer] }

qos multicast egress-max-buffer port {
[guaranteed_max_buffer][best-effort_max_buffer] }
```

Enabling PVST+ support

NOTE
The following changes are made to the Enabling PVST+ support section in the Configuring Spanning Tree Protocol chapter of the *Brocade MultiService IronWare Switching Configuration Guide*.

Existing content:

If you want a tagged port to also support IEEE 802.1Q BPDUs, you need to enable the dual-mode feature on the port. The dual-mode feature is disabled by default and must be enabled manually.

Modified content:

The tagged port also supports IEEE 802.1Q BPDUs, since the dual-mode feature on the port is enabled, by default.

Assigning or changing a VLAN priority

The following note is modified in the Configuring port-based VLANs section in the VLANs chapter of the *Brocade Multi-Service Ironware Switching Configuration Guide*.

NOTE
When you apply the VLAN priority command with running traffic, it may drop packets for a short period of time and flush out the MAC addresses. This is normal behavior.

Specifying the number of MAC addresses to be denied

The following content is added to the "Using the MAC Port Security Feature" chapter of the *Multi-Service IronWare Security Configuration Guide* under the "Configuring the MAC port security feature" section.

Specifying the number of MAC addresses to be denied

You can specify the number of MAC addresses that are to be denied before the NetIron device shuts the port down using the **restrict-max-deny** command.

```
Brocade(config)# interface ethernet 7/11
Brocade(config)# interface ethernet 7/11
Brocade(config-if-e100-7/11)# port security
Brocade(config-if-e100-7/11)# violation restrict
Brocade(config-port-security-e100-7/11)# restrict-max-deny 40
```

Syntax: restrict-max-deny *number*

The *number* parameter indicates the number of MAC addresses that are to be denied before the NetIron device shuts the port down. The *number* range is between 1 and 1024. The code example indicates that the device will be shut down after 40 MAC addresses are denied.

NTP loss of sync message

The NTP Loss of Sync message has been updated to include the last synchronized device source.

```
May 25 04:27:18:I:NTP: The system clock is not synchronized to any time source.
Last synchronized to 20.67.50.10. The reference time is 04:25:09.2387832160 GMT+05
Sun May 25 2014
```

Path selection metric for CSPF computation

The IGP floods two metrics for every link when the MPLS traffic engineering (TE) is configured in a network. The two metrics are the OSPF or the IS-IS link metric and a TE link metric. To optimize the use and performance of the network, it is always better to identify specific tunnels to carry data traffic and voice traffic. This implementation allows you to specify tunnel path selection to the requirements of each type of traffic. For example, certain tunnels are to carry voice traffic (which requires low delay) and other tunnels are to carry data (where delay is acceptable).

The path calculation metric implementation allows you to specify the path calculation for a given tunnel based on either of the following requirements:

- IGP link metric for path calculation for data traffic
- TE link metric for path calculation for voice traffic

The current implementation of RSVP-TE uses the IGP metric value of the TE-links to compute CSPF path for the LSPs and does not allow configuring TE-metric explicitly. With this enhancement, users are allowed to configure TE metric value at the MPLS interface level. The decision of whether to use TE-metric or IGP-metric for CSPF computation by the LSPs is determined by CLI configurations at two levels:

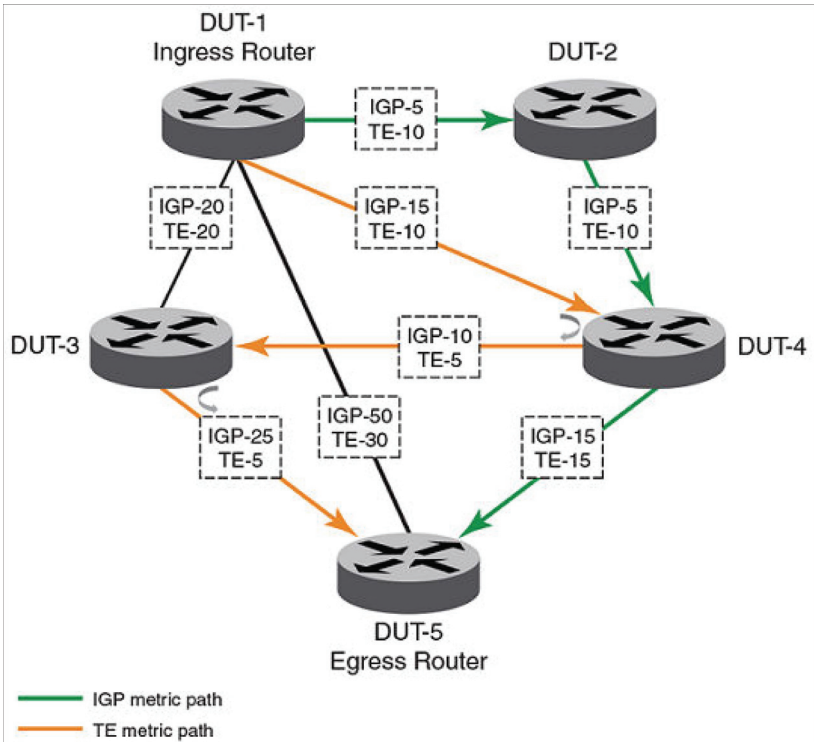
- Global level: This configuration covers all RSVP LSPs (primary, secondary, static bypass, and dynamic bypass LSPs).
- Individual LSP level: This configuration covers all RSVP LSPs except dynamic bypass which needs to be configured per MPLS interface level

NOTE
The CLI configuration at the LSP level always overrides the configuration at the global level. That is, the decision to use te-metric or igp-metric for CSPF path calculation if configured at the LSP level, always overrides the configuration at the global level.

Path selection for CSPF computation

The selection of path for the LSP depends on whether you want to use IGP or TE metric for CSPF computation. Consider the network topology in the illustration. The ingress router is DUT 1 and the egress router is DUT 5. There are two cases depending upon whether IGP metric or TE metric is used for CSPF computation.

FIGURE 1 Path Selection for CSPF computation



When IGP metric is selected

The LSP selects the following path:

- DUT1 --> DUT2 --> DUT4 --> DUT5

When TE metric is selected

The LSP selects the following path:

- DUT1 --> DUT4 --> DUT3 --> DUT5

Configuring TE-metric for MPLS interface

To configure TE-metric for a MPLS interface, you must perform the following steps.

1. Enable traffic engineering under router mpls policy to OSPF or ISIS.
2. Configure the MPLS interface.
3. Set the te-metric value at the MPLS interface or leave it as a default value to use the igp-metric value of the te-links for CSPF computation (optional).

NOTE
By default, all LSPs use global configuration.

Configuring the CSPF computation mode

To configure the CSPF computation mode on a device, you must perform the following steps.

1. Set the cspf-computation mode under router mpls policy to use te-metric or igp-metric at the global level.
2. Enable or disable cspf-computation mode to use te-metric or igp-metric locally at the LSP level for primary, secondary, and bypass LSPs or at the MPLS interface level in the case of dynamic bypass LSPs. (optional)

NOTE
By default, all LSPs use global configuration.

Configuring TE-metric for an interface

You can configure the TE metric value at a specified MPLS interface level. Note that traffic engineering needs to be enabled at the router policy level.

```
Brocade(config-mpls)# mpls-interface eth 1/1
Brocade(config-mpls-if-e1000-1/1)# te-metric 5
Brocade(config-mpls-if-e100-1/1)#no te-metric 3
Error:TE-metric is configured to a value of 5
Brocade(config-mpls-if-e100-1/1)#no te-metric 5
```

In the example, the TE-metric is set back to a default value of IGP-metric. Run the **show mpls interface ethernet 1/1** command to view the configured value.

NOTE
If **te-metric** uses the default value or if the **no** form of the command is used, **te-metric** will be equal to **igp-metric** value in the MPLS TE database.

Configuring the CSPF computation mode value at global level

You can configure the cspf-computation mode at the global level under the router mpls policy.

```
Brocade(config-mpls)# policy
Brocade(config-mpls-policy)#cspf-computation-mode ?
use-bypass-metric use bypass LSP's path cost for selection between bypass LSP's
use-igp-metric use IGP metric of the link for CSPF computation use-te-metric use
TE metric of the link for CSPF computation
Brocade(config-mpls-policy)#cspf-computation-mode use-igp-metric
Brocade(config-mpls-policy)#no cspf-computation-mode use-te-metric
Error:CSPF computation is configured to use igp-metric
Brocade(config-mpls-policy)#no cspf-computation-mode use-igp-metric
```

In the example, the CSPF computation mode is set back to a default value of te-metric. Run the **show mpls policy** command to view the configured value.

NOTE
The use-bypass-metric and the **use-igp-metric** or **use-te-metric** options can be enabled simultaneously.

Configuring the CSPF computation mode value for primary LSPs

You can configure the cspf-computation-mode value at the primary LSP level.

By default, the LSP uses the global configuration at the router mpls policy. If explicitly configured, the configuration at the LSP level always overrides the configuration at the global level.

```
Brocade(config)# router mpls
Brocade(config-mpls)# lsp test
Brocade(config-mpls-lsp-test)#cspf-computation-mode ?
use-igp-metric use IGP metric of the link for CSPF computation
use-te-metric use TE metric of the link for CSPF computation
Brocade(config-mpls-lsp-test)# cspf-computation-mode use-igp-metric
Brocade(config-mpls-policy)#no cspf-computation-mode use-te-metric
Error:CSPF computation is configured to use igp-metric
Brocade(config-mpls-policy)#no cspf-computation-mode use-igp-metric
```

In the example, the CSPF computation mode is set back to a default value of te-metric. Run the **show mpls lsp detail** command to view the configured value.

NOTE
The configuration is not an adaptive parameter and another instance is not created when the configuration is changed on the fly for adaptive LSPs but on re-optimization it takes up the new configuration to perform cspf computation.

Configuring the CSPF computation mode value for secondary LSPs

You can configure the cspf-computation-mode value at the secondary LSP level.

By default, the LSP uses the global configuration at the router mpls policy. If explicitly configured, the configuration at the LSP level always overrides the configuration at the global level.

```
Brocade(config)# router mpls
Brocade(config-mpls)# lsp test
Brocade(config-mpls-lsp-test)#secondary-path 12
Brocade(config-mpls-lsp-secpath-12)#cspf-computation-mode ?
use-igp-metric use IGP metric of the link for CSPF computation use-te-metric use
TE metric of the link for CSPF computation
Brocade(config-mpls-lsp-test-secpath-12)# cspf-computation-mode use-te-metric
```

In the example, the CSPF computation mode is set back to a default value of te-metric. Run the **show mpls lsp detail** command to view the configured value.

Configuring the CSPF computation mode value for static bypass LSPs

You can configure the cspf-computation-mode value at the static bypass LSP level.

By default, the LSP uses the global configuration at the router mpls policy. If explicitly configured, the configuration at the LSP level always overrides the configuration at the global level.

```
Brocade(config)# router mpls
Brocade(config-mpls)# bypass-lsp b1
Brocade(config-mpls-bypasslsp-b1)#cspf-computation-mode ?
use-igp-metric use IGP metric of the link for CSPF computation
use-te-metric use TE metric of the link for CSPF computation
Brocade(config-mpls-bypasslsp-b1)# cspf-computation-mode use-te-metric
```

Run the **show mpls lsp detail** command to view the configured value.

Configuring the CSPF computation mode value for dynamic bypass LSPs

You can configure the cspf-computation-mode for dynamic bypass LSPs at the mpls-interface level.

By default, the LSP uses the global configuration at the router mpls policy. If explicitly configured, the configuration at the LSP level always overrides the configuration at the global level.

```
Brocade(config)#router mpls
Brocade(config-mpls)#mpls-interface eth 1/15
Brocade(config-mpls-if-e1000-1/15)#dynamic-bypass
Brocade(config-mpls-if-e1000-1/15-dynamic-bypass)#cspf-computation-mode ?
use-igp-metric use IGP metric of the link for CSPF computation
use-te-metric use TE metric of the link for CSPF computation
Brocade(config-mpls-if-e1000-1/15-dynamic-bypass)#cspf-computation-mode
use-te-metric
```

Run the **show mpls dynamic-bypass interface detail** command to view the configured value.

No advertising of inter-vrf-leaked routes out to L3VPN

When a route is imported from one VRF to another VRF using inter-vrf route leaking feature, the imported route in the destination VRF can be redistributed into VRF-BGP. It can also be advertised out to L3VPN network.

The advertised L3VPN route originally imported from a different VRF will use the export route-target(s) from the destination VRF.

This feature will not automatically block inter-vrf leaked routes from being advertised out to L3VPN network. To block inter-vrf leaked routes use the no version of the command.

The default behavior is backward compatible. A BGP option has been added to disable backward compatibility.

Syntax: [no] export-vrf-leaked-routes

The default is **export-vrf-leaked-routes** enabled.

Routes are not autocratically blocked. To block inter-vrf leaked routes use the **no** version of the command.

This feature is compatible with NetIron R05.6.00d.

```
router bgp
local-as 100
…
Brocade(config)# address-family vpnv4 unicast
Brocade(config)# export-vrf-leaked-routes
Brocade(config)# exit-address-family

Brocade(config)# address-family vpnv6 unicast
Brocade(config)# export-vrf-leaked-routes
Brocade(config)# exit-address-family

end of BGP configuration
```

AES-CTR encryption mode support for SSH

The Advanced Encryption Standard - Cipher Block Chaining (AES-CBC) encryption mode for Secure Shell (SSH) is vulnerable to certain plain-text attacks. AES-CTR mode support has been added to avoid the vulnerability. The support for encryption algorithms such as aes256-ctr, aes128-ctr are available.

1. The Advance encryption standard modes has been reordered to provide preference to CTR mode over CBC mode on SSH connection.
2. The CBC mode support is available for backward compatibility with existing SSH clients that only support CBC mode.

NOTE
The AES-CTR mode must be configured both on the client and server sides to establish an SSH connection.

2x100G XPP ILKN Monitoring

The 2x100G XPP ILKN monitoring feature will monitor CRC errors in the Interlaken link / interface between XPP1 and XPP2 in 2 packet processors for the 2x100G card.

In 2x100G cards, CRC errors on the Interlaken link between iXPP1 and iXPP2 in the packet processor result in packet drops. The 2x100G XPP ILKN monitoring feature will generate syslog and SNMP traps if software reads more than configured drops on ILKN links between iXPP1 and iXPP2. Syslog and SNMP traps display the number of packet drops in the Interlaken interface and CRC errors in lane groups.

Two 100G ports are available. For each port:

- One XPP (with two internal ingress XPPs, iXPP1, iXPP2, and an egress XPP) is present to perform packet processing. This feature polls for Interlaken errors between ingress XPPs, iXPP1, and iXPP2.
- Two identical CXPP1x100G packet processors are present to perform 200Gbps packet processing.

SYSLOG and SNMP traps are generated if packet drops result from CRC errors in the Interlaken link / interface between iXPP1 and iXPP2. The affected ports are shutdown if the Interlaken link / interface was configured through the new CLI configuration command based on the following factors:

- The option to shutdown the affected ports is configured using the new global configuration command.
- The option to disable the feature is configured using the new global configuration command.

Syslog and SNMP traps are generated once the packets drop are seen because of Interlaken CRC errors. The syslog/SNMP trap is generated once every 3 minutes with the following information:

- Indicating the number of packet drops and CRC errors in each lane group.
- Indicating if ports are not disabled by the port shut down option.

sysmon np interlaken-monitor

The global configuration command sysmon np interlaken-monitor {crc-port-shutdown | disable} is used to shut down available 100G ports if drops in the ILKN interface are more than the configured number of drops (crc-port-shutdown); or disable the feature (disable).

Syntax: sysmon np interlaken-monitor crc-port-shutdown

Syntax: no sysmon np interlaken-monitor crc-port-shutdown

Syntax: sysmon np interlaken-monitor disable

Syntax: no sysmon np interlaken-monitor disable

By default, the feature is enabled to poll ILK2 DROP COUNT register 0x200f4 every 30 seconds, and if there are 10 drops or more on ILK2 DROP COUNT register 0x200f4, then syslog and SNMP traps are generated.

Parameters

crc-port-shutdown Port shutdown option is set globally for all the 2x100G cards available in the MLX. The crc-port-shutdown global configuration command will be used to shut down the available 100G ports if the drops in ILKN interface are more than the configured number of drops. (No command is available to disable the port shutdown option.)

disable Interlaken monitoring feature is disabled globally for all the 2x100G cards available in the MLX. The disable global configuration command will be used to disable the feature. This command will be used disable the feature in all LP's across resets. (No command is available to enable the Interlaken monitoring option for all the 2x100 LPs available in the MLX.)

Examples

The port shutdown option is set.

```
Brocade (config)#sysmon np interlaken-monitor crc-port-shutdown
```

The Interlaken monitoring feature is disabled in all LPs.

```
Brocade (config)#sysmon np interlaken-monitor disable
```

The show interface Ethernet <slot/port> CLI command will display the reason for port down as Interlaken CRC error.

```
Brocade (config)#show int e 1/1
    100GigabitEthernet1/1 is down(interlaken crc error), line protocol is down STP
    Root Guard is disabled, STP BPDU Guard is disabled
    NP transmitted 0 packets, Received from TM 0 packets
```

The **show sysmon config** command will display the configuration details for ILKN CRC monitoring. Action is none by default. If sysmon np Interlaken-monitor crc-port-shutdown is configured, action will be displayed as DISABLE-PORTS. Mode will be displayed as POLLING by default and if the feature is disabled, then it will displayed as DISABLED. Poll period will display the value as 30 seconds, which is the global default configuration for this feature.

```
Brocade (config)#show sysmon config
-----------------------+-------+-------------------------+----------+----------
+------------+-----------------+--------------------
EVENT   |ACTION|SLOTS         |MODE   | POLL PERIOD | THRESHOLD |LOGBACK-OFF| |
|                               | (SEC)        | #(PER POLL||| | in #POLL)| |
-----------------------+--------+-------------------------+-------------
+-------------------+-------------------+--------------------
NP ILKN   |NONE     | BR-MLX-100Gx2 |POLLING     | 30 | N/A  N/A Monitoring
```

Chapter

2

Documentation updates for Multi-Service IronWare Diagnostic Guide

In this chapter

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

NOTE
There are no updates for NetIron 5.6.00b.

NOTE
There are no updates for NetIron 5.6.00c.

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

CPU memory show commands

NOTE
The following section corrects typographical error from double fees to double frees, as stated below.

show bm-dump-mode

Syntax: show bm-dump-mode

Use the **show bm-dump-mode** command to pinpoint offending code that may be responsible for double frees and memory leaks. Command output resembles the following example.

```
Brocade# show bm-dump-mode
Buffer dump mode is enabled
```

NOTE
A track state of 0 means that the buffer was allocated before the show bm-dump-mode command was executed.

NOTE
There are no updates for NetIron 5.6.00e.

NOTE
There are no updates for NetIron 5.6.00f.

Chapter

Documentation updates for Unified IP MIB Reference 3

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.

TABLE 8

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. • 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	Specifies all images upgrade. • 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 NetIron XMR and the Brocade MLX Series. For Brocade NetIron CES and Brocade NetIron CER series, only the monitor, application, and FPGA images are upgraded. Returns false(2), for a read-only operation. Default: false(2)
brcdSwIntfModAutoUpgradeAllImages brcdIp.1.1.2.16.1.2.5 Syntax: TruthValue	Read-write	Specifies all images upgrade. • The upgrade sequence includes only the LP boot image, if set to true(1). • The default false(2), upgrades only the LP FPGA images. Returns false(2), for a read-only operation. **NOTE:** This object is deprecated. SET operation is not supported and READ operation will return false(2).

Upgraded MIB Objects

The following two MIB objects have been added to trap MIB for Multi-Service IronWare Release 05.6.00e.

Name, OID, and syntax	Access	Description
snTrapNPILKNCRCError brcdIp.1.1.2.16.1.0.1113 Syntax: snAgGblTrapMessage	Read-write	The SNMP trap that is generated when packet drops are observed in 2x100G ports because of Interlaken CRC errors.
snTrapARPMACMovement brcdIp.1.1.2.16.1.0.1114 Syntax: snAgGblTrapMessage	Read-write	The SNMP trap that is generated when the MAC address associated with a host IP is changed.

Chapter 4

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.

PBIF Recovery

In rare cases, the LP CPU might not be able to send packets because of a lockup in the PCI Bus Interface FPGA (PBIF). If this happens, all control protocols (such as OSPF, VRRP, etc) will go down and traffic will be affected. To recover from this situation, the LP has to be reloaded. By default, the system will perform this recovery automatically. This behavior can be changed using the **no system-monitoring pbif lp-reset-recovery** command.

Syntax

Syntax: system-monitoring pbif lp-reset-recovery

Syntax: no system-monitoring pbif lp-reset-recovery

Command Default

This command is enabled by default i.e., the system will reset the LP when PBIF locks up.

Examples

To **deactivate automatic** PBIF recovery perform the **`no system-monitoring pbif lp-reset-recovery`** command.

```
Brocade# config
Brocade(config)# no system-monitoring pbif lp-reset-recovery
Brocade(config)# exit
Brocade# write memory
Brocade# reload
```

Router modules

NOTE

Starting with the 5.6.00a code release, XMR-32, MLX-32, and MLXe-32 systems will support a maximum of 25 NI-MLX-1GX48-T-A modules. If more than 25 NI-MLX-1GX48-T-A modules are currently installed in these systems and the code is upgraded to any NetIron patch or software release later than 5.6.00 from a pre-5.6.00 NetIron release, the system will no longer recognize the remaining NI-MLX-1GX48-T-A modules. It is recommended that these excess modules are removed from the system and all references to these slots are removed from the startup configuration prior to upgrading to any 5.6.00 patch release.

TX drain support

When a Brocade MLX Series or Brocade NetIron XMR device is upgraded to software releases NetIron 5.4.00e and above, incrementing CRC errors might be observed on neighboring device ports connected to the Brocade MLX Series or Brocade NetIron XMR device, when flow control is triggered.

TX drain support has been added to allow packets to drain in TX at the MAC level. When a port goes down or is in the idle state the TX drain will drain the packets.

The TX drain is now configured based on port UP/DOWN event there by taking care of PAUSE frames and LF/RF and avoid CRC errors

tx_drain_disable bit in MAC_control_register (0x0300) is

Set to 1 when port is enabled

Set to 0 when port is disabled

By default tx_drain_disable bit is set to 0

NOTE
When tx_drain is not configured, CRC errors and traffic drop are seen when PAUSE frames or local/remote faults happen on the interface.

The following modules for Brocade MLX Series or Brocade NetIron XMR device running 5.4.00e and above are affected.

- NI-MLX-10Gx8-M
- NI-MLX-10Gx8-D
- BR-MLX-10Gx8-X
- RW2_20X10GE_X
- BR-MLX-100Gx2-CFP2
- RW2_4X40GE
- BR-MLX-10Gx4-M-IPSEC