14 November 2018

NetIron OS 6.3.00a for ExtremeRouting MLX Series Devices

Release Notes v1.0

Contents

Document history 5

Preface 6

Contacting Extreme Technical Support 6

Extreme resources 6

Document feedback 7

Overview 8

Behavior changes 9

Behavior changes in release NetIron 6.3.00a 9

Software Features 10

New software features introduced in R6.3.00 10

CLI commands 11

New CLI commands NetIron R6.3.00 11

MIBs and messages 12

MIBs 12

Messages 12

RFCs and standards 13

Hardware support 14

Supported devices 14

Supported devices for Network Packet Broker R6.3.00a 15

Supported modules 16

Supported power supplies 22

Supported optics 22

Software upgrade and downgrade 23

Image file names 23

Migration path 33

Upgrade and downgrade considerations 33

Limitations and restrictions 38

Important notes 38

Defects 40

TSBs—Critical issues to consider prior to installing this release 40

Closed with code changes NI6.3.00a 41

Closed with code changes NI6.3.00 42

Closed without code changes NI6.3.00 74
Known issues NI6.3.00 80

Document history

Version	Summary of changes	Publication date
1.0	Initial release	11/14/2018

Preface

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for immediate support
- Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
- Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at https://www.extremenetworks.com/support/documentation/ .

Document feedback

Quality is our first concern at Extreme, 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.

You can provide feedback in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/
- Email us at documentation@extremenetworks.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Overview

NetIron OS Release 6.3.00 enhances the capabilities of ExtremeRouting MLX Series, and ExtremeRouting CER 2000 Series in the following areas:

* BGP services,

* Network Packet Broker functionality

In addition, this release also has further enhancements to manageability and troubleshooting functions to enable efficient network operations.

With these features, the MLX Series Router continues as the leading platform for converged data center and service provider network services.

Behavior changes

Behavior changes in release NetIron 6.3.00a

There are no behavior changes in release NetIron 6.3.00a.

Software Features

NOTE: The NetIron 6.3.00 release (the image files and the documentation) is no longer available from the Extreme Portal. New software features introduced in release 6.3.00 are included in release 6.3.00a.

New software features introduced in R6.3.00

The following software features are introduced in NetIron 6.3.00 release.

Management features and enhancements

- **SSH server management**: This feature configures the SSH server to allow incoming SSH connection requests from ports that belong to any VRF and from the out-of-band management port when the management VRF is configured.
- **Increase maximum telnet session number from 5 to 10:** The maximum telnet session is increased from 5 to 10.

Security

- **Regular expression support in RADIUS command authorization**: The Extreme-specific RADIUS attribute `foundry-command-string` now supports specifying a range of data for a CLI command.

IP Routing

- **BGP Large Communities:** RFC8092 BGP Large Communities attribute is supported. All routes with this attribute belong to the communities specified in the attribute.
- **Increase number of loopback interfaces in NetIron to 1024:** The number of supported loopback interfaces is increased to 1024.

Monitoring

- Beginning with Extreme NetIron Release 6.3.00a, the Network Processor (NP) error monitoring and recovery feature is supported on Extreme NetIron 8x10G, 2x100G, 20x10G, 2x100G-CFP2 and 4x10G-IPSEC line card modules for ExtremeRouting XMR/MLX Series.

Network Packet Broker

- The maximum TVF LAG FID group size (system-max tvf-lag-lb-fid-group) is increased to 32.

CLI commands

New CLI commands NetIron R6.3.00

- ip large-community-list extended
- ip large-community-list standard
- ip ssh include-all-vrf
- match large-community-list
- set large-community
- set large-community-list
- system-max loopback-interface
- show default values
- show ip bgp routes large-community
- show ip bgp routes large-community-access-list
- show ip bgp routes large-community-regex
- show ip bgp routes detail large-community
- show ip bgp routes detail large-community-access-list
- show ip bgp routes detail large-community-regex

Modified commands

- ip ssh strict-management-vrf
- neighbor send-community
- show ip ssh config
- show who
- system-max tvf-lag-lb-fid-group

Deprecated commands

There are no deprecated commands in this release.

MIBs and messages

MIBs

New MIB Objects

No MIB objects were introduced in release NetIron 6.3.00a.

Modified MIBs

The following MIBs have been modified for this release:

Not Applicable

Deprecated MIBs

The following MIBs have been deprecated beginning with this release:

Not Applicable

Messages

New Messages

The following messages are new in this release:

Not Applicable

Modified Messages

The following messages have been modified for this release:

Not Applicable

Deprecated Messages

The following messages have been deprecated beginning with this release:

- Not Applicable

RFCs and standards

The following new RFC is supported in this release.

- RFC8092 -- BGP Large Communities Attribute

Hardware support

Supported devices

The following devices are supported in this release:

NOTE: Beginning with NetIron OS 6.3.00a and later, the ExtremeSwitching CES 2000 Series devices are not supported. Refer to the End of Sale and End of Support page for additional information.

ExtremeRouting XMR Series	ExtremeRouting MLX Series	ExtremeRouting CER 2000 Series
XMR 4000	MLX-4	CER-RT 2024C-4X
XMR 8000	MLX-8	CER-RT 2024F-4X
XMR 16000	MLX-16	CER 2024C
XMR 32000	MLX-32	CER-RT 2024C
	MLXe-4	CER 2024F
	MLXe-8	CER-RT 2024F
	MLXe-16	CER 2048C
	MLXe-32	CER-RT 2048C
		CER 2048CX
		CER-RT 2048CX
		CER 2048F
		CER-RT 2048F
		CER 2048FX
		CER-RT 2048FX

Supported devices for Network Packet Broker R6.3.00a

XMR Series	MLX Series
XMR 4000	MLX-4
XMR 8000	MLX-8
XMR 16000	MLX-16
XMR 32000	MLX-32
	MLXe-4
	MLXe-8
	MLXe-16
	MLXe-32

Supported modules

The following interface modules are supported in this release:

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-10GX4-IPSEC-M	MLX 4-port 10 GbE/1 GbE combo and 4-port 1 GbE (-M) IPsec module with 512,000 IPv4 routes or 240,000 IPv6 routes in hardware	Yes	Yes	3
BR-MLX-10GX20-X2	MLX 20-port 10 GbE/1 GbE (X2) SFP+ and SFP combo module with extended route table support for up to 2.4 million IPv4 or 1.8 million IPv6 routes in hardware. Integrated hardware-enabled MACsec.	Yes	Yes	3
BR-MLX-10GX20-M	MLX 20-port 10 GbE/1 GbE (M) combo module. Supports SFP+ and SFP with up to 512,000 IPv4 routes or 240,000 IPv6 routes in FIB. Integrated hardware-enabled MACsec.	Yes	Yes	3
BR-MLX-1GCX24-X-ML	MLX 24-port (X) 10/100/1,000 copper (RJ-45) module with IPv4/IPv6/MPLS hardware support. Supports 512,000 IPv4 routes in FIB. License upgradable to “X” scalability (1 million IPv4 routes in hardware).	Yes	No	1.1

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-100GX2-CFP2-M	MLX 2-port 100 GbE (M) CFP2 module. Supports 512,000 IPv4 routes in FIB.	Yes	Yes	3
BR-MLX-100GX2-CFP2-X2	MLX 2-port 100 GbE (X2) CFP2 module with extended route table support for up to 2.4 million IPv4 or 1.8 million IPv6 routes in hardware.	Yes	Yes	3
BR-MLX-10GX8-X	MLX Series 8-port 10 GbE (X) module with IPv4/IPv6/MPLS hardware support—requires SFP optics. Supports up to 1 million IPv4 routes in FIB. Requires high-speed switch fabric modules.	Yes	Yes	2
BR-MLX-1GCX24-X	MLX 24-port (X) 10/100/1,000 copper (RJ-45) module with IPv4/IPv6/MPLS hardware support. Supports 1 million IPv4 routes in hardware.	Yes	Yes	1.1

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-40GX4-M	MLX Series 4-port 40 GbE (M) module with IPv4/IPv6/MPLS hardware support and support for QSFP+ optics, including both LR and SR versions. Supports up to 512,000 IPv4 routes or 128,000 IPv6 routes. Requires high-speed switch fabric modules.	Yes	Yes	3
BR-MLX-10GX4-X	MLX Series 4-port 10 GbE (X) module with IPv4/IPv6/MPLS hardware support—requires XFP optics. Supports 1 million IPv4 routes in hardware.	Yes	Yes	1.1
BR-MLX-10GX4-X-ML	MLX/MLXe 4-port 10 GbE (ML) module with IPv4/IPv6/MPLS hardware support—requires XFP optics. Supports 512,000 IPv4 routes in FIB. License upgradable to "X" scalability (1 million IPv4 routes in hardware).	Yes	No	1.1
NI-MLX-10GX8-M	MLX Series 8-port 10 GbE (M) module with IPv4/IPv6/MPLS hardware support and up to 512,000 IPv4 routes—requires SFP+ optics and high-speed switch fabric modules.	Yes	No	2

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-1GFX24-X	MLX Series 24-port FE/GbE (SFP) module, with IPv4/IPv6/MPLS hardware support. Supports 1 million IPv4 routes in hardware.	Yes	Yes	1.1
BR-MLX-1GFX24-X-ML	MLX Series 24-port FE/GbE (SFP) module, with IPv4/IPv6/MPLS hardware support. Supports 512,000 IPv4 routes in FIB. License upgradable to "X" scalability (1 million IPv4 routes in hardware).	Yes	No	1.1
BR-MLX-10GX24-DM	MLXe 24-port 10 GbE module with IPv4/IPv6/MPLS hardware support—requires SFP optics. Supports 256,000 IPv4 routes in FIB.	Yes	No	3a
NI-MLX-10GX8-D	MLX Series 8-port 10-GbE (D) module with IPv4/IPv6 hardware support - requires SFPP optics. Supports 256K IPv4 routes in FIB. Does not support MPLS. Requires high speed switch fabric modules.	Yes	No	2

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-10GX10-X2	MLX 10-port 10-Gbe/1Gbe (X2) SFP+ and SFP combo module with extended route table support up to 2M IPv4 and 800K IPv6 routes in hardware. MACsec enabled. Upgradeable to 20X10G-X2 using additional software license.	Yes	Yes	3
BR-MLX-1GX20-U10G-M	MLXe twenty (20)-port 1-GBE/1-GBE (M) module with IPv4/IPv6/MPLS hardware support. Requires SFP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules. Upgradeable to 10G, with BR-MLX-1GX20-U10G-MUPG license.	Yes	Yes	3

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-1GX20-U10G-X2	MLXe twenty (20)-port 1-GBE (X2) module with IPv4/IPv6/MPLS hardware support. Requires SFP optics. Supports simultaneous 2M IPv4 and 0.8M IPv6, or 1.5M IPv4 and 1M IPv6 routes in FIB. Requires hSFM. Upgradeable to 10G with extra license.	Yes	Yes	3

- Depending on your router model, you can install up to 32 single-slot interface modules, or 16 double-slot interface modules.
- Interface modules are hot-swappable. Interface modules can be removed and replaced without powering down the system.
- Gen 3 - X2 modules with an MR2-M module will only support 512M routes.

Supported power supplies

The following table lists the power supplies that are available for the devices supported in this release:

Part number	Description	Compatible devices
BR-MLXE-ACPWR-1800	1800W power supply.	16-, 8- and 4-slot MLXe and 16 and 8-Slot XMR/MLX AC
BR-MLXE-DCPWR-1800	1800W power supply.	16-, 8- and 4-slot MLXe and 16 and 8-Slot XMR/MLX DC
NI-X-ACPWR	1200W power supply.	16-, 8- and 4-slot MLXe and 16 and 8-Slot XMR/MLX AC
NI-X-DCPWR	1200W power supply.	16-, 8- and 4-slot MLXe and 16 and 8-Slot XMR/MLX DC
NI-X-ACPWR-A	1200W power supply.	4-Slot XMR/MLX AC
NI-X-DCPWR-A	1200W power supply.	4-Slot XMR/MLX DC
BR-MLXE-32-ACPWR-3000	AC 3000W power supply.	32-slot MLXe/XMR/MLX
BR-MLXE-32-DCPWR-3000	DC 3000W power supply.	32-slot MLXe/XMR/MLX
NIBI-32-ACPWR-A	AC 2400W power supply.	32-Slot MLXe/XMR/MLX
NIBI-32-DCPWR	2400W power supply.	32-Slot MLXe/XMR/MLX DC

Supported optics

For a list of supported fiber-optic transceivers that are available from Extreme, refer to the latest version of the Extreme Optics Family Data Sheet available online at https://cloud.kapostcontent.net/pub/a070d154-d6f1-400b-b2f0-3d039ae2f604/data-center-ethernet-optics-data-sheet?kui=Cc1YBpmqyfb2mDfw2vlq2g.

Software upgrade and downgrade

Image file names

Download the following images from www.extremenetworks.com.

NOTE: Beginning with NetIron OS 6.3.00a and later, the ExtremeSwitching CES 2000 Series devices are not supported. Refer to the End of Sale and End of Support page for additional information.

MLX Series and NetIron XMR devices

NOTE: When upgrading MLX Series and XMR Series devices, follow the manifest upgrade to ensure all required files are upgraded. Boot upgrade is not part of the manifest upgrade. If the boot image is R05.6.00 or older, upgrade the boot image.

Required images for R6.3.00a MLX Series/XMR software upgrade

```
# Manifest File for XMR/MLX Release 06.3.00

-NETIRON_IRONWARE_VER XMR-MLXV6.3.00a

#====================================================================

-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin

-DIRECTORY /Boot/ManagementModule
xmprm05900.bin

#  Application Images
-DIRECTORY /Combined/FPGA
lpfpga06300a.bin

-DIRECTORY /Combined/Application
xm06300a.bin

-DIRECTORY /Monitor/InterfaceModule
xmlb06200.bin

-DIRECTORY /Monitor/ManagementModule
xmb06200.bin

-DIRECTORY /Application/ManagementModule
xmr06300a.bin

-DIRECTORY /Application/InterfaceModule
xmlp06300a.bin
```

```
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06300a.bin 2.11
pbif8x10_06300a.bin 2.24
pbifmrj_06300a.bin 4.04
pbifsp2_06300a.bin 4.02
statsmrj_06300a.bin 0.09
xgmacsp2_06300a.bin 0.17
xpp2x100_06300a.bin 1.06
xpp4x40_06300a.bin 6.20
xpp4x10g3_06300a.bin 0.00
xpp8x10_06300a.bin 1.10
xppmrj_06300a.bin 1.03
xppsp2_06300a.bin 1.01
xppxsp2_06300a.bin 1.01
pbif-ber-g3_06300a.bin 2.11
xpp20x10g3_06300a.bin 0.00
xpp2x100g3_06300a.bin 0.00
-DIRECTORY /FPGA/ManagementModule
mbridge32_06300a.xsvf 36
mbridge_06300a.xsvf 37
sbridge_06300a.mcs 6
hsbridge_06300a.mcs 17
-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06200.sig
xmb06200.sig
xmr06300a.sig
xmlp06300a.sig
lpfpga06300a.sig
hsbridge_06300a.sig
mbridge_06300a.sig
mbridge32_06300a.sig
sbridge_06300a.sig
pbif4x40_06300a.sig
pbif8x10_06300a.sig
pbifmrj_06300a.sig
pbifsp2_06300a.sig
pbif-ber-g3_06300a.sig
statsmrj_06300a.sig
xgmacsp2_06300a.sig
xpp2x100_06300a.sig
xpp20x10g3_06300a.sig
xpp2x100g3_06300a.sig
xpp4x40_06300a.sig
xpp4x10g3_06300a.sig
xpp8x10_06300a.sig
xppmrj_06300a.sig
xppsp2_06300a.sig
```

```
xppxsp2_06300a.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06200.sha256
xmb06200.sha256
xmr06300a.sha256
xmlp06300a.sha256
lpfpga06300a.sha256
hsbridge_06300a.sha256
mbridge_06300a.sha256
mbridge32_06300a.sha256
sbridge_06300a.sha256
pbif4x40_06300a.sha256
pbif8x10_06300a.sha256
pbifmrj_06300a.sha256
pbifsp2_06300a.sha256
pbif-ber-g3_06300a.sha256
statsmrj_06300a.sha256
xgmacsp2_06300a.sha256
xpp2x100_06300a.sha256
xpp20x10g3_06300a.sha256
xpp2x100g3_06300a.sha256
xpp4x40_06300a.sha256
xpp4x10g3_06300a.sha256
xpp8x10_06300a.sha256
xppmrj_06300a.sha256
xppsp2_06300a.sha256
xppxsp2_06300a.sha256
```

FPGA file names and supported modules

File Name	Supported Modules
pbif4x40_06300a.bin	4x40G modules
pbif8x10_06300a.bin	8x10G modules
pbifmrj_06300a.bin	24x1G and 48x1G modules
pbifsp2_06300a.bin	2x10G, 4x10G, 4x10G-x and 20x1G modules
statsmrj_06300a.bin	24x1G and 48x1G modules
xgmacsp2_06300a.bin	2x10G, 4x10G-x and 4x10G modules
xpp2x100_06300a.bin	2x100G modules (double-wide CFP-based module)
xpp4x40_06300a.bin	4x40G modules
xpp4x10g3_06300a.bin	4x10G modules
xpp8x10_06300a.bin	8x10G modules
xppmrj_06300a.bin	24x1G and 48x1G modules
xppsp2_06300a.bin	2x10G, 4x10G, and 20x1G modules
xppxsp2_06300a.bin	4x10G-x

pbif-ber-g3_06300a.bin	20x10G and 2x100G modules (-M and –X2)
xpp20x10g3_06300a.bin	20x10G modules
xpp2x100g3_06300a.bin	2x100G modules (half-slot CFP2-based module)
mbridge32_06300a.xsvf	MBRIDGE32
mbridge_06300a.xsvf	MBRIDGE
sbridge_06300a.mcs	Switch fabric modules
hsbridge_06300a.mcs	High speed switch fabric modules

CER 2000 Series devices

When upgrading CER 2000 Series devices, follow the manifest upgrade to ensure all required files are upgraded. Boot upgrade is not part of the manifest upgrade. If the boot image is R05.5.00 or older, upgrade the boot image.

Required images for R6.3.00a CER 2000 software upgrade

```
-NETIRON_IRONWARE_VER CES-CERV6.3.00a
#=====================================================================
-DIRECTORY /Boot
ceb06000.bin

-DIRECTORY /Application
ce06300a.bin

-DIRECTORY /FPGA
pbifmetro_06300a.bin

-END_OF_IMAGES

-DIRECTORY /Signatures
ceb06000.sig
ce06300a.sig
pbifmetro_06300a.sig
ceb06000.sha256
ce06300a.sha256
```

pbifmetro_06300a.sha256

-DIRECTORY /MIBS

ce06300a.mib

ce06300a_std.mib

-DIRECTORY /Yang

ExampleXML.txt

common-defs.yang

interface-config.yang

interface-statedata.yang

mpls-config.yang

mpls-statedata.yang

netiron-config.yang

netiron-statedata.yang

version-statedata.yang

vlan-config.yang

vlan-statedata.yang

-DIRECTORY

CES-CER06300a_mnf.txt

CES-CER06300a_mnf.sig

CES-CER06300a_mnf.sha256

-DIRECTORY /Manuals

Manifest for Network Packet Broker devices

NOTE: When upgrading MLX Series and XMR Series devices, follow the manifest upgrade to ensure all required files are upgraded. Boot upgrade is not part of the manifest upgrade. If the boot image is R05.6.00 or older, upgrade the boot image.

Required images for Network Packet Broker R6.3.00a software upgrade

```
-NETIRON_IRONWARE_VER XMR-MLXV6.3.00a
#====================================================================
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin

-DIRECTORY /Boot/ManagementModule
xmprm05900.bin

#  Application Images
-DIRECTORY /Combined/FPGA
lpfpga_npb_06300a.bin

-DIRECTORY /Combined/Application
xm06300a.bin

-DIRECTORY /Monitor/InterfaceModule
xmlb06200.bin

-DIRECTORY /Monitor/ManagementModule
xmb06200.bin

-DIRECTORY /Application/ManagementModule
xmr06300a.bin

-DIRECTORY /Application/InterfaceModule
xmlp06300a.bin
```

```
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06300a.bin 2.11
pbif8x10_06300a.bin 2.24
pbifmrj_06300a.bin 4.04
pbifsp2_06300a.bin 4.02
statsmrj_06300a.bin 0.09
xgmacsp2_06300a.bin 0.17
xpp2x100_06300a.bin 1.06
xpp4x40_06300a.bin 6.20
xpp4x10g3_06300a.bin 0.00
xpp8x10_06300a.bin 1.10
xppmrj_06300a.bin 1.03
xppsp2_06300a.bin 1.01
xppxsp2_06300a.bin 1.01
pbif-ber-g3_06300a.bin 2.11
xpp20x10g3_npb_06300a.bin 0.10
xpp2x100g3_npb_06300a.bin 0.10

-DIRECTORY /FPGA/ManagementModule
mbridge32_06300a.xsvf 36
mbridge_06300a.xsvf 37
sbridge_06300a.mcs 6
hsbridge_06300a.mcs 17

-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
```

xmlb06200.sig

xmb06200.sig

xmr06300a.sig

xmlp06300a.sig

lpfpga_npb_06300a.sig

hsbridge_06300a.sig

mbridge_06300a.sig

mbridge32_06300a.sig

sbridge_06300a.sig

pbif4x40_06300a.sig

pbif8x10_06300a.sig

pbifmrj_06300a.sig

pbifsp2_06300a.sig

pbif-ber-g3_06300a.sig

statsmrj_06300a.sig

xgmacsp2_06300a.sig

xpp2x100_06300a.sig

xpp20x10g3_npb_06300a.sig

xpp2x100g3_npb_06300a.sig

xpp4x40_06300a.sig

xpp4x10g3_06300a.sig

xpp8x10_06300a.sig

xppmrj_06300a.sig

xppsp2_06300a.sig

xppxsp2_06300a.sig

xmlprm05900.sha256

xmprm05900.sha256

xmlb06200.sha256

xmb06200.sha256

xmr06300a.sha256

```
xmlp06300a.sha256
lpfpga_npb_06300a.sha256
hsbridge_06300a.sha256
mbridge_06300a.sha256
mbridge32_06300a.sha256
sbridge_06300a.sha256
pbif4x40_06300a.sha256
pbif8x10_06300a.sha256
pbifmrj_06300a.sha256
pbifsp2_06300a.sha256
pbif-ber-g3_06300a.sha256
statsmrj_06300a.sha256
xgmacsp2_06300a.sha256
xpp2x100_06300a.sha256
xpp20x10g3_npb_06300a.sha256
xpp2x100g3_npb_06300a.sha256
xpp4x40_06300a.sha256
xpp4x10g3_06300a.sha256
xpp8x10_06300a.sha256
xppmrj_06300a.sha256
xppsp2_06300a.sha256
xppxsp2_06300a.sha256

#  MIBS:
-DIRECTORY /MIBS
xmr06300a.mib
xmr06300a_std.mib

-DIRECTORY /Yang
ExampleXML.txt
```

```
common-defs.yang
interface-config.yang
interface-statedata.yang
mpls-config.yang
mpls-statedata.yang
netiron-config.yang
netiron-statedata.yang
version-statedata.yang
vlan-config.yang
vlan-statedata.yang

-DIRECTORY /Tools
sbsupgrd.zip

-DIRECTORY
MLX_npb_06300a_mnf.txt
MLX_npb_06300a_mnf.sig
MLX_npb_06300a_mnf.sha256

-DIRECTORY /Manuals
```

FPGA file names for NPB and supported modules

File Name	Supported Modules
xpp20x10g3_npb_06300a.bin	20x10G modules FPGA for NPB
xpp2x100g3_npb_06300a.bin	2x100G modules (half-slot CFP2-based module) FPGA to NPB

Migration path

To establish an appropriate migration path from your current release of Extreme NetIron, consult your Extreme TAC representative (see the Preface of this document).

Upgrade and downgrade considerations

To upgrade to NetIron 6.3.00a, a two-step approach may be required.

Scenario 1

Customers running releases 05.9.00a, 05.6.00ga, 05.6.00h, 05.8.00d, 05.7.00e or subsequent releases can directly upgrade to NetIron 6.3.00a.

NOTE: If you are not running one of the releases listed above, you CANNOT directly upgrade to 6.3a.

Scenario 2

To upgrade from 05.6.00c or any later release (other than the images mentioned in Scenario 1), a two-step approach is required.

1. Upgrade to 05.9.00a or any of the following releases: 05.6.00ga, 05.6.00h, 05.8.00d, 05.7.00e or subsequent patch releases and reload the device.

2. Upgrade to NetIron 6.3.00a. Reload the device.

Scenario 3

To upgrade to NetIron 6.3.00a from releases prior to R05.6.00c, a two-step approach is required.

1. Upgrade to 5.9.00a or any of the following releases: 05.6.00ga, 05.6.00h, 05.8.00d or 05.7.00e and reload the device.

2. Upgrade again to the same image which was used in step 1 and reload the device again. This ensures that the device will have the SHA256 signatures on the device if they are needed, for example for LP Auto-upgrade.

3. Upgrade to NetIron 6.3.00a and reload the device.

Scenario 4

Use Scenario 4 if you want to use the following features specific to the NPB FPGA.

- VxLAN header stripping
- GTP de-encapsulation
- Packet Timestamping
- Source port labeling
- NVGRE stripping
    - NetIron 6.3.00a UDA Enhancements

1. Upgrade to NetIron 6.3.00a using any of above scenarios based on the image from which the upgrade is being performed.
2. Reload the device again and verify that the system is up with NetIron 6.3.00a.
3. Configure the **fpga-mode-npb** command and save the configuration.
4. Upgrade to the NetIron 6.3.00a NPB image using MLX_npb_6300a_mnf.txt and reload the device.
5. Make sure BR-MLX-10Gx20 and BR-MLX-100Gx2-CFP2 have NPB XPP images.
6. Verify the system. Check the output of the **show version** command and the **show flash** command to make sure the image versions are correct. Check the output of the **show module** command to make sure the line cards are not in Interactive state due to FPGA mismatch. Interactive state is an error state due to FPGA mismatch.

Show output examples

The following examples provide excerpts of the command output.

Output example for the show version command

```
SSH@MLX8-PE1#show version
System Mode: MLX
...
...
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SL 3: NI-MLX-10Gx8-M 8-port 10GbE (M) Module (Serial #: BEQ0427H04G, Part #:
60-1001587-16)
(LID: dgsFJHMjFJi)
Boot     : Version 5.9.0T175 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900
(449576 bytes) from boot flash
Monitor  : Version 6.2.0T175 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200
(573366 bytes) from code flash
IronWare : Version 6.3.0T177 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Aug 27 2018 at 18:26:50 labeled as xmlp06300
(9572782 bytes) from Primary
FPGA versions:
Valid PBIF Version = 2.24, Build Time = 4/7/2016 14:16:00

Valid XPP Version = 1.10, Build Time = 2/7/2017 10:41:00
```

Output example for the show flash command

```
SSH@MLX8-PE1#show flash
```

```
...
...
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 1
Code Flash: Type MT28F256J3, Size 66846720 Bytes (~64 MB)
  o IronWare Image (Primary)
    Version 6.3.0T177, Size 9572782 bytes, Check Sum 93f3
    Compiled on Aug 27 2018 at 18:26:50 labeled as xmlp06300
  o IronWare Image (Secondary)
    Version 5.7.0bT177, Size 7800332 bytes, Check Sum 5d75
    Compiled on Oct 22 2014 at 20:08:46 labeled as xmlp05700b
  o Monitor Image
    Version 6.2.0T175, Size 573366 bytes, Check Sum faad
    Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200
Boot Flash: Type MX29LV040C, Size 512 KB
  o Boot Image
    Version 5.9.0T175, Size 449576 bytes, Check Sum 3bc9
    Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900
FPGA Version (Stored In Flash):
 PBIF Version = 2.11, Build Time = 8/19/2016 14:54:00

XPP Version = 0.00, Build Time = 5/9/2017 17:31:00
```

Output example for the show module command

```
MCT2#show module

Module                                                    Status
                Ports    Starting MAC

M1 (left ):BR-MLX-MR2-X Management
Module                        Active

M2 (right):BR-MLX-MR2-X Management Module                 Standby(Ready
State)

F1: NI-X-HSF Switch Fabric
Module                                Active

F2: NI-X-HSF Switch Fabric
Module                                Active

F3: NI-X-HSF Switch Fabric
Module                                Active

S1: BR-MLX-10Gx8-X 8-port 10GbE (X)
Module                       CARD_STATE_UP               8        0024.38a4.9
200

S2: BR-MLX-10Gx20 20-port 1/10GbE
Module                         CARD_STATE_UP              20       0024.38a4
.9230

S3: BR-MLX-40Gx4-M 4-port 40GbE
Module                           CARD_STATE_UP             4        0024.38
a4.9260
```

```
S4: BR-MLX-100Gx2-CFP2 2-port 100GbE
Module                      CARD_STATE_UP               2        0024.38a4.92
90
```

OpenFlow upgrade and downgrade

When downgrading the system from NetIron 6.3.00a to NetIron 05.8.00, if there are any VRF interfaces which are enabled with OpenFlow, some unexpected IFL entries will be seen after moving to R05.8.00. These unexpected IFL entries may affect the L3VPN/6VPE traffic.

Extreme recommends removing OpenFlow from the VRF interfaces before downgrading the router to R05.8.00 For upgrade and migration considerations, refer to the latest version of the Extreme NetIron Software Upgrade Guide.

Hitless upgrade support

Hitless Upgrade is supported from R6.3.00 to R6.3.00a.

Limitations and restrictions

Important notes

Saving system information to flash

- This feature is not supported on Gen1 LPs.

Support for Management IP as snmp trap-source

- IPV6 support is not present currently for trap source addresses.

ACL/PBR co-existence with Openflow on same port

- PBR/ACL is not supported on L23 openflow hybrid port.
- L2 PBR/ACL is not supported on L3 openflow hybrid port.
- L3 PBR/ACL is not supported on L2 openflow hybrid port.
- L2 ACL Deny logging is not supported openflow hybrid port.

RADIUS Over Transport Layer Security (TLS)

- Dot1x accounting is not supported over RADSEC/TLS.

IPv6 ACL based rate limit for CES/CER

- ACL based rate limit is supported only on physical interface.

SCP based simplified upgrade

- This is not supported on CES/CER devices.
- This feature is supported on MR2 management modules.
- Feature is supported from 5.7 and above version.
- The signature verification is performed when the firmware version is 6.1.
- Verification supported only when pre-upgrade version on device is NetIron 6.1 and above.

OpenFlow group table

- The only action allowed in action bucket is output port.
- Each action bucket can have only one output port.
- Maximum of 8 buckets are allowed in an OpenFlow group with logical ports.
- Group types All, Indirect and Fast-Failover are not supported for logical port groups. Only SELECT group type will be supported.
- Bucket statistics is not supported.
- Group cannot have physical port and logical port in the buckets. Either physical ports or logical ports should be present.
- Modification of a group with all physical ports to all logical ports in the buckets and vice versa are not supported.
- Generic OpenFlow rule with action logical port group is not supported.
- This feature is not supported in CES/R.

- Logical port group along with actions other than L2VPN/L3VPN label in flow action are not supported.

VLAN modification in MPLS egress

- Pop VLAN action is limited to OpenFlow hybrid ports as output in action.
- In a dual tagged packet, only modification of outer VLAN is supported and addition/deletion of outer VLAN he inner VLAN modification/addition/deletion are not supported.

SCP checksum, firmware integrity

- The signature verification is not performed for copying LP application, monitor to specific slot using TFTP , Slot1/Slot2 and LP boot using from Slot1/Slot2

IPv6 ACL Scaling 4k Enhancement is supported only on XMR /MLX Series·

LDP interface transport address

- LDP interface transport address should not be enabled when there are multiple parallel adjacencies (interfaces) present between the LDP routers. If user wishes to enable this feature then they should remove the additional adjacencies. If a user enables this feature with multiple adjacencies to a peer then it is possible that the interface transport address may not be used and/or the session would be torn down due to role conflict.
- Pre-requisites: Enabling LDP interface transport address feature on the interface (adjacency) will cause any existing session to flap and come back up with interface IP address as transport address (only in cases where there is a single adjacency between the peers). This can be service impacting and something the user should be well aware of before executing the command.

Defects

TSBs—Critical issues to consider prior to installing this release

Technical Support Bulletins (TSBs) provide detailed information about high priority defects or issues present in a release. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific release. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. TSBs can be found at https://extremeportal.force.com/ (note that TSBs are generated for all Extreme platforms and products, so not all TSBs apply to this release).

TSB issues resolved in NI 6.3.00a

TSB	Summary
None	

TSB issues outstanding in NI 6.3.00a

TSB	Summary
None	

Closed with code changes NI6.3.00a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 11/09/2018 in NetIron OS 6.3.00a.

Defect ID:	DEFECT000667280		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	BGP4 - IPv4 Border Gateway Protocol
Reported In Release:	NI 06.3.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	A peer BGP router terminates a BGP session with 'Malformed Attribute List' error		
Condition:	Re-advertising routes that are received with "unknown" attributes		
Workaround:	1. Look for 'Malformed" BGP packets on the peer router side and identify the prefixes with 'Malformed Attribute List'. 2. Define a BGP prefix-list filter to filter out these prefixes on the inbound side from where the prefixes are learned from		

Closed with code changes NI6.3.00

NOTE: The NetIron 6.3.00 release (the image files and the documentation) is no longer available from the Extreme Portal. New software features introduced in release 6.3.00 are included in release 6.3.00a.

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 08/30/2018 in NetIron OS 6.3.00.

Defect ID:	DEFECT000628768		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	"show dai" CLI output showing DHCP snooping entries with null port information for interfaces where DHCP snooping is disabled		
Condition:	(1) configure a VE interface through which DHCP clients are configured and DHCP snooping is enabled (2) configure a second VE interface on which DHCP clients are connected through a DHCP relay agent, but DHCP snooping is not enabled (3) configure another VE interface on which DHCP server resides		

Defect ID:	DEFECT000642455		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.6.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Standby Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 203afea4: nht_get_specific_index_from_pool(pc) 203b31fc: nht_create_new_entry_standby(lr) 203b31fc: nht_create_new_entry_standby 203b3d38: nht_standby_mp_update_entry 203b56a4: nht_standby_mp_process_dy_messages 2033a738: process_dy_change_packet 2032192c: ipc_process_messages 20322600: ipc_receive_packet 20f3cc70: sw_receive_packet 20f3d778: mp_rx_main 00005e18: sys_end_task		

Condition:	It is observed rarely on a MLX/XMR device with OSPF, VRRP or MPLS combination

Defect ID:	DEFECT000644574		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF neighbors may show all ECMP paths after upgraded MLXe fails setting a forwarding address in AS External LSA.		
Condition:	It is rarely observed with the following steps:- (1) OSPFv2 is enabled on the device (2) static routes are configured with gateway, which is reachable and redistributed into OSPFv2 (3) Repeated image upgrade and downgrade		
Recovery:	Flapping the interface towards the gateway will resolve the issue.		

Defect ID:	DEFECT000645700		
Technical Severity:	Low	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 05.8.00	**Technology:**	Sysmon
Symptom:	Execution of "sysmon sfm walk status" command may not return to command prompt		
Condition:	Execution of "sysmon sfm walk status" from telnet or ssh		
Workaround:	Execute "sysmon sfm walk status" from console session		
Recovery:	A return key will help		

Defect ID:	DEFECT000646227		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 05.8.00	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Link may go down with Brocade 100G-LR4 CFP2 optic		
Condition:	Rarely observed when a interface is disabled and then enabled with Brocade 100G-LR4 CFP2 optic having serial number starting from YDF		

Defect ID:	DEFECT000646510		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Monitoring

Reported In Release:	NI 06.0.00	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Unable to configure "speed-duplex 100-full" on CES/CER 1G port		
Condition:	On Optics E1MG-100BXD and E1MG-100BXU		

Defect ID:	DEFECT000646724		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Traffic drop due to increase in BGP convergence time		
Condition:	1. The device has both BGP/OSPF configuration 2. BGP has (iBGP/eBGP) neighborship with more than 50 neighbor of routers with multiple policies configured for RIB-Out processing 3. OSPF is used as IGP for installing the BGP routes 4. OSPF path changes by cost modifications or port down events		

Defect ID:	DEFECT000649540		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 05.6.00	**Technology:**	IP over MPLS
Symptom:	Connectivity may be lost for 3 minutes when backup LSP path is down		
Condition:	1.The problematic prefix has to be learned from two different BGP peers. 2.Both BGP peers should have equal IGP cost 3.Static NULL0 drop route also configured for the next-hop 4.Backup LSP path is down		
Workaround:	Configure route-maps with MED to override the Static NULL0 route		

Defect ID:	DEFECT000649776		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Management Module module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20adcd84: cu_optic_process_cfp_aggregate_optical_mon_parameter(pc) 20ade1e8: cu_get_aggregate_optical_parameter_from_object(lr) 20ade1e8: cu_get_aggregate_optical_parameter_from_object 208a98b4: snIfOpticalMonitoringInfoEntry_get_value 208a9e2c: snIfOpticalMonitoringInfoEntry_next 209642f4: SNMP_Process_Bulk_Redo 20966fb4: SNMP_Continue_function 20967088: process_packet_two 2096751c: process_packet_one 20967868: Process_Rcvd_SNMP_Packet_Async 20965504: Process_Received_SNMP_Packet 209919a4: snmp_receive_message 209943a0: snmp_udp_recv_callback_common 209944ac: snmp_udp_recv_callback 20ba0540: itc_process_msgs_internal 20ba09ec: itc_process_msgs 2099101c: snmp_task 00005e18: sys_end_task		
Condition:	While inserting non-Brocade (Flex Optix) CFP2-QSFP28 adapter on a 2x100G-CFP2 Linecard module		

Defect ID:	DEFECT000649996		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	VRRP-E session state changes unexpectedly		
Condition:	Polling SNMP table: lldpRemTable (.1.0.8802.1.1.2.1.4.1)		
Workaround:	Disable SNMP polling for the table: lldpRemTable (.1.0.8802.1.1.2.1.4.1)		

Defect ID:	DEFECT000650682		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.6.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF ECMP route for some of external destinations may not be installed into the routing table of non-translator NSSA ABR.		
Condition:	(1) Atleast two NSSA ABRs present in the OSPF network (2) About 100 or so external destinations are redistributed into NSSA area by two NSSA ASBRs with FA set to an address within the NSSA area.		

Defect ID:	DEFECT000651122		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Line card module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20f0839c: fpip_process_pending_packets(pc) 20f08398: fpip_process_pending_packets(lr) 20f039d0: fpip_update_host_cache_entry 20f03b4c: fpip_update_host_cache_in_all_vrf 20f19544: arp_process_one_entry_pram_update 20d1e178: lp_cam_update_arp_entry_pram 20e23fb0: process_one_arp_update_lp 20f176ec: process_one_arp_update 20f17950: process_arp_dy_messages 20bd5818: process_dy_change_packet 20c1ca54: ipc_multi_module_handler 20c1efc8: ipc_process_messages 20c1f7a4: ipc_receive_packet 20036ce4: ge_process_ipc_data_msg 207f4f20: lp_ipc_task 00040158: sys_end_task		
Condition:	It is rarely observed during a Line card bootup or a link flap between MCT clusters		

Defect ID:	DEFECT000651855		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.0.00	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	2x100G-CFP2 Linecard module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 00069064: assert_dobule_free_large_memory(pc) 0006905c: assert_dobule_free_large_memory(lr) 00069274: free_memory_pool 00069918: free_memory 00065e80: dev_free_memory 00005024: xsyscall 2000105c: free 21610cb8: bcm_pm_if_cleanup 20026928: bcm_82790_uninit 209cd328: phy_adapter_removed 209b946c: phy_conn_check_existence 20a4086c: port_read_physical_existance 20a309ec: port_check_port_status 20a34900: port_link_status_poll 20a34404: port_status_poll 200058c0: perform_callback 200062c8: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f3af4: main 00040158: sys_end_task		
Condition:	While removing a non-Brocade (Flex Optix) CFP2-QSFP28 adapter from the 2x100G-CFP2 Line card module		

Defect ID:	DEFECT000651862		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.1.00	**Technology:**	IP Addressing
Symptom:	Traffic loss might be observed on MLX with Q-in-Q configuration		
Condition:	1. MRP should be configured on outer VLAN of Q-in-Q 2. Physical loopback connection should be established between two interfaces where one interface belongs to outer VLAN and other interface belongs to inner VLAN of Q-in-Q		

Defect ID:	DEFECT000651950		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	CLI - Command Line Interface
Symptom:	Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 54797064: (pc) 20ac71d8: cu_show_int_lag_callback(lr) 20ad8e04: cu_show_int_lag 2044cc58: show_int_lag_all 202e8754: call_action_func 202e924c: parse_node 202e8cc8: parse_node_recurse 202e9514: parse_node 202e8cc8: parse_node_recurse 202e9514: parse_node 2035cd28: parse_input 2041c358: cli_aaa_accounting_callback 207906c0: aaa_accounting_start 2041bbac: cli_request_command_accounting 202e913c: parse_node 202e7790: parser 2035cd04: parse_input 20a94a74: ssh_event_handler 20aa7ccc: ProcessChannelData 20aa52e8: ShProcessMessage 20aae688: ProcessClientInputData 20aade20: ShFiniteStateMachine 209b03cc: HandleProtocolAction 209b01ac: HandleConnectionTask 20a93644: ssh_connection_task 20a93d90: ssh_socket_control 20a96a2c: ssh_receive_data_ready 20a96a70: ssh_tcp_receive_data_ready_callback 20b9321c: itc_process_msgs_internal 20b936c8: itc_process_msgs 20a8edc0: ssh_in_task 00005e18: sys_end_task		
Condition:	"Show interface lag" is executed frequently from one or more SSH sessions		

Defect ID:	DEFECT000652160		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	CLI - Command Line Interface
Symptom:	Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 202e3aec: generic_map_put(pc) 20bb6784: mplp_get_lp_data_request(lr) 20bb6784: mplp_get_lp_data_request 20ba0540: itc_process_msgs_internal 20ba09ec: itc_process_msgs 20bb8020: lp_agent_task 00005e18: sys_end_task		
Condition:	"Show interface lag" is executed frequently from one or more SSH sessions		

Defect ID:	DEFECT000652191		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.0.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	MAC table synchronization may not be complete for MCT cluster nodes		
Condition:	Line card module goes into a rolling reboot for any known/other reasons		

Defect ID:	DEFECT000653000		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	IPv6 Addressing
Symptom:	IPV6 neighbor stuck in PROBE state		
Condition:	1. Connect the host with MLX and establish neighbors 2. Remove connected host 3. IPV6 entries are not removed and stuck in PROBE state		
Recovery:	clear ipv6 neighbors		

Defect ID:	DEFECT000653092		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 06.0.00	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	MPLS BFD session which has multiple path will go down and comes up		
Condition:	During LSP path switch BFD session will go down after 60 seconds and comes up. This happens only for adaptive LSPs		

Defect ID:	DEFECT000653095		
Technical Severity:	Low	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 06.0.00	**Technology:**	MPLS Traffic Engineering
Symptom:	Sometimes when executing "show tech-support mpls" some of the commands would not show output, instead they'll show a message "invalid input -> mpls"		
Condition:	For show rsvp session in "show tech-support mpls"		

Defect ID:	DEFECT000654961		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 05.9.00	**Technology:**	Traffic Queueing and Scheduling
Symptom:	Traffic loss may be observed with LAG		
Condition:	After boot up of any Gen1.1 line card in the presence of LAG configurations		
Recovery:	Undeploy and deploy of LAG		

Defect ID:	DEFECT000655172		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 05.8.00	**Technology:**	Hardware Monitoring
Symptom:	The 'show chassis' may display incorrect information for available power and power status fields		
Condition:	Power-off power supply manually (OR) Remove and re-insert the power cord.		

Defect ID:	DEFECT000656069		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.6.00	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	Traffic loss may be observed with VRRP		
Condition:	VRRP has to be configured on virtual interface and physical port is part of Un tagged VLAN This is applicable for CES/CER devices only.		

Defect ID:	DEFECT000656359		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.1.00	**Technology:**	CLI - Command Line Interface
Symptom:	Following error message may be observed on LP Console kbp_duplicate_entry_IPVPN[0] idx : 0x00218021 tbl_id : 32 vpn_id = 4097, pfx : a.b.c.d/32		
Condition:	1. Configure CAM in amod mode 2. Configure a loopback interface 3. Configure a VRF in VE interface 4. Remove and re-add VRF in VE interface		

Defect ID:	DEFECT000656781		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP may display a maximum number 4294967295 when polled for this object fdryVplsEndPoint2InnerTag		
Condition:	VPLS endpoints are configured with no inner tag		

Defect ID:	DEFECT000656819		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.2.00	**Technology:**	CLI - Command Line Interface
Symptom:	The 'show optic' command may display optic data as N/A even though the port is up like below:- MLX2#sh optic 1 Port Temperature Tx Power Rx Power Tx Bias Current +----+----------+----------+----------+----------+ 1/1 N/A N/A N/A N/A 1/2 N/A N/A N/A N/A		
Condition:	1. Line card module is 20x10G. 2. Dual mode optic is connected and speed is configured as 1G. 3. Line card is reloaded with 1G speed configuration.		
Recovery:	The only recovery to correct the display issue is to reset line card by following below steps:- 1. Remove 1G configuration and reload line card module. 2. After boot up reapply the configuration.		

Defect ID:	DEFECT000657495		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	SNMP polling may display incorrect information for BGP peer's session UP time		
Condition:	Polling this Object "bgpPeerFsmEstablishedTime" through SNMP		

Defect ID:	DEFECT000657519		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	IPv6 Addressing
Symptom:	Following IPV6 CAM Update violations may be observed with high CPU on Line Card module:- Nov 8 16:37:06:A:CAM update violation: slot 3 XPP 2 0x000abcdef 0x00000000		
Condition:	Very rarely observed during frequent modifications of IPV6 routes		

Defect ID:	DEFECT000657929		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.2.00	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	OSPFv3 Interface number may not be displayed correctly in "show log" output like below:- Nov 30 05:22:15:N:OSPFv3: Interface state changed, rid a.b.c.d, intf eth x/y, state down, where x/y is not correct physical port/interface		
Condition:	Enable/Disable OSPFv3 interface followed by the execution of "show ipv6 ospf neighbors"		

Defect ID:	DEFECT000658040		
Technical Severity:	High	**Probability:**	High
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.1.00	**Technology:**	IPsec - IP Security
Symptom:	IPsec tunnel session would not come up.		
Condition:	This could happen when the IPsec configuration on a linecard module is out of sync with the management module.		
Recovery:	Reload the LC may recover from the problem. If not, reload of the system will be required.		

Defect ID:	DEFECT000658072		
Technical Severity:	Low	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.0.00	**Technology:**	PBR - Policy-Based Routing
Symptom:	GTP-u packet with L3 header as IPV4 and L4 header as IPv6 not forwarded with the IPv6 PBR on GTP port		
Condition:	Configure IPv6 PBR and enable ingress-inner-filter on GTP port		
Workaround:	Configure any IPv4 PBR with IPv6 PBR and bind it to the same GTP port		

Defect ID:	DEFECT000658203		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	Configuration Fundamentals
Symptom:	Management Module may reload unexpectedly with the following stack trace:- Exception Type 1100 (DTLB Load), telnet_0 0008f030: msr 00000000: dar 00000000: dsisr 202ed8dc: next_token(pc) 202f0af8: parse_node(lr) 202f0af8: parse_node 202f04f0: parse_node_recurse 202f0d3c: parse_node 202f04f0: parse_node_recurse 202f0d3c: parse_node 20364838: parse_input 2042a7e0: cli_aaa_accounting_callback 2079f290: aaa_accounting_start 2042a034: cli_request_command_accounting 202f0964: parse_node 202eefb8: parser 20364814: parse_input 20a90aac: handle_new_line_from_telnet_client 20a91408: telnet_application_control 20a94814: telnet_receive_packet 20a93240: telnet_socket_control 20a97ee0: telnet_receive_data_ready 20a97f24: telnet_tcp_receive_data_ready_callback 20ba3844: itc_process_msgs_internal		
Condition:	1. 'aaa accounting commands 0 default start-stop' is configured 2. Debug destination is set to TELNET 3. 'no telnet server' is issued on the same TELNET session		

Defect ID:	DEFECT000658216		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 05.4.00	**Technology:**	CLI - Command Line Interface
Symptom:	Active Management Module may unexpectedly reload with the following stack trace:- 2018052c: print_prompt(pc) 2017d6e0: print_prompt(lr) 2031f718: prompt_and_reprint 20390ac4: internal_release_page_mode 20390c2c: release_page_mode 2038fa90: parse_input 2094b848: ssh_event_handler 2095a0e8: ProcessChannelData 20958304: ShProcessMessage 2095f664: ProcessClientInputData 2095eed8: ShFiniteStateMachine 208845a0: HandleProtocolAction 20884d84: HandleReceive 20884ca4: HandleWaitingForReceive 20884448: HandleConnectionTask 2094a5bc: ssh_connection_task 2094ad3c: ssh_socket_control 2094d4b4: ssh_receive_data_ready 2094d4f8: ssh_tcp_receive_data_ready_callback 20a24f54: itc_process_msgs_internal 20a2528c: itc_process_msgs 20946a04: ssh_in_task 00005e18: sys_end_task		
Condition:	Configure "ntp-interface ve? command for VE interface id with higher value		

Defect ID:	DEFECT000658409		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP doesn't advertise component routes after applying the 'unsuppress-map' configuration		
Condition:	(1) BGP configured with 'router bgp' command (2) 'aggregate-address' command configured to advertise the summary route for all the component routes that fall within the summary address (3) Configure component routes with network command and apply the unsuppress-map command to the neighbors for which component routes need to be advertised		
Recovery:	Remove and reconfigure 'aggregate-address x.x.x.x summary-only? command followed by the execution of `clear ip bgp neighbor all? or device reload.		

Defect ID:	DEFECT000658414		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.0.00	**Technology:**	SSH - Secure Shell
Symptom:	SSH Authentication may fail sometimes		
Condition:	with RSA public key authentication		

Defect ID:	DEFECT000658728		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 05.8.00	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	Line card may reload unexpectedly with the following stack trace:- Possible Stack Trace (function call return address list) 20f75174: traverse_all_ports_for_local_interface(pc) 20f75084: traverse_all_ports_for_local_interface(lr) 20df9abc: lp_vpls_dy_sync_tlv_port_config 20df7050: lp_vpls_dy_sync_tlv_process_dy_messages 20bb6718: process_dy_change_packet 20bfba30: ipc_multi_module_handler 20bfdcf0: ipc_process_messages 20bfe4b0: ipc_receive_packet 20034390: ge_process_ipc_data_msg 207eeac8: lp_ipc_task 00040158: sys_end_task		
Condition:	1. Port has to be configured as a tagged port in the VPLS VLAN 2. Delete the port from the VPLS VLAN using this CLI "no tagged eth <slot/port>"		

Defect ID:	DEFECT000658936		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 05.8.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP task may cause High CPU		
Condition:	polling the OIDs of the tables .ipNetToPhysicalTable.(1.3.6.1.2.1.4.35) and .ipNetToMediaTable.(1.3.6.1.2.1.4.22)		

Defect ID:	DEFECT000658954		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 06.0.00	**Technology:**	Traffic Queueing and Scheduling
Symptom:	Protocols may flap when configured with very low timeout value less than or equal to 100 msec and Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 0002f89c: get_memory_pool_info(pc) 00005024: xsyscall(lr) 000b6558: set_memory_histogram 0002e140: allocate_memory_pool 0002ed40: allocate_memory 0002b124: dev_allocate_memory 00005024: xsyscall 203105d0: os_malloc_zero 20b9eda0: itc_alloc_request_state 20b9f10c: itc_send_request_internal 20ba0f20: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 205490a8: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 205490a8: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 205490a8: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 20549104: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper		

	20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 20549104: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 20549104: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 20549104: show_tm_non_empty 20037eec: show_tech_support 2035ed7c: timer_callback_wrapper 20ba069c: itc_process_msgs_internal 20ba0f44: itc_send_request_and_wait_internal 20ba14e8: itc_send_request_and_wait 20f1a22c: bfd_scb_send_itc 20549104: show_tm_non_empty 20037eec: show_tech_support Call stack too deep!
Condition:	1. UDLD is configured with 100ms timeout by configuration command 'link-keepalive interval 1' 2. when any one of the following command is executed 'show tech', 'show tm non-empty-queues' or 'show tm non-empty-queues detail'
Workaround:	Increase the Protocol timer expiry value accordingly.

Defect ID:	DEFECT000659364		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	static routes may not be advertised into BGP		
Condition:	1. BGP neighborship is established with the neighbor 2. "filter-change-update-delay 0" is configured 3. static routes are configured and redistributed into BGP 4. reload the chassis		
Recovery:	clear ip route a.b.c.d/x		

Defect ID:	DEFECT000659434		
Technical Severity:	Medium	**Probability:**	High
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.0.00	**Technology:**	Hardware Monitoring
Symptom:	A 10G interface runs at 1G speed		
Condition:	Specific to 20x10G line card when a port is configured for loop back system		

Defect ID:	DEFECT000659435		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.2.00	**Technology:**	ACLs - Access Control Lists
Symptom:	IPv6 ACL accounting doesn't include PBR routed packets		
Condition:	Configure IPv6 PBR with the set clause as "interface null0"		

Defect ID:	DEFECT000659530		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	SDN
Reported In Release:	NI 06.2.00	**Technology:**	OpenFlow
Symptom:	Layer2/3 OpenFlow could not be enabled on a interface from BVM tool and the following error message will be observed:- Error: Port x/y is not untagged member in default VLAN 1		
Condition:	changing the port configuration from OpenFlow enable Layer 3 to Layer 2 or vice versa from BVM tool		

Defect ID:	DEFECT000659772		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.0.00	**Technology:**	Hardware Monitoring
Symptom:	Fiber Version of CES/CER may power down		
Condition:	Very rarely switch models of NI CER-2024F-4X and NI CES-2024F-4X may power down and doesn't come UP		
Workaround:	Configure the following fan-threshold parameters. CES2024F-4X#show fan-threshold === Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_CPU) === Fan Speed Low: -1 - 52 Fan Speed Med: 48 - 56 Fan Speed Med-Hi: 53 - 60 Fan Speed Hi: 57 - 90 max_ts_shut_off_count = 1 shut_off_count = 0 0 === Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_PPCR1) === Fan Speed Low: -1 - 52 Fan Speed Med: 48 - 56 Fan Speed Med-Hi: 53 - 60 Fan Speed Hi: 57 - 100 max_ts_shut_off_count = 1 shut_off_count = 0 0 === Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_PPCR2) === Fan Speed Low: -1 - 52 Fan Speed Med: 48 - 56 Fan Speed Med-Hi: 53 - 60 Fan Speed Hi: 57 - 100 max_ts_shut_off_count = 1 shut_off_count = 0 0 === Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_PPCR3) === Fan Speed Low: -1 - 52 Fan Speed Med: 48 - 56 Fan Speed Med-Hi: 53 - 60 Fan Speed Hi: 57 - 100 max_ts_shut_off_count = 1 shut_off_count = 0 0		

Defect ID:	DEFECT000660056		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.0.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	LAG Load balancing may not be observed for GTP-c packets		
Condition:	1) GTP has to be enabled on the port 2) GTP-c TEID hashing should be enabled		

Defect ID:	DEFECT000660088		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Line card may reload unexpectedly with the following stack trace:- Possible Stack Trace (function call return address list) 21672168: memcpy(pc) 211fe30c: kbp_memcpy(lr) 20b5bf9c: kbp_npxxpt_compare_data 20b5b504: kbp_npxxpt_execute_req 20b5b300: kbp_npxxpt_service_reqs 21547c34: kbp_xpt_service_requests 21546500: kbp_dm_12k_cbwlpm 2152ca78: device_compare 2152dcd0: kbp_instruction_search 21599064: NlmNsTrie__CheckAndFixRpt 215990f8: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599180: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries		

	21599190: NlmNsTrie__FindRptEntries 215992d4: NlmNsTrie__SearchAndRepairRpt 215a7988: kbp_ftm_search_and_repair_rpt 215881bc: kbp_lpm_db_advanced_search_and_repair 215bab14: kbp_device_advanced_fix_errors 21534f38: kbp_device_12k_fix_parity_errors 2152a538: kbp_device_fix_errors 20b5561c: netroute_ifsr_fix_errors 20ac956c: nlcam_ifsr_netroute_scan_errors 20ac8b90: nlcam_ifsr_fifo_poll 200058c0: perform_callback 200062c8: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f3af4: main 00040158: sys_end_task
Condition:	Rarely observed during the execution of 'clear BGP neighbor' command when software is trying to fix a CAM error at the same time
Workaround:	To disable soft repair feature through CLI 'cam ifsr disable'

Defect ID:	DEFECT000660187		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.4.00	**Technology:**	IP Addressing
Symptom:	Management port accepts packets corresponding to the same subnet of the lowest IPv4 primary address only		
Condition:	On configuring multiple IPv4 primary address on management port		

Defect ID:	DEFECT000660397		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	Routes through dead DR Other Router stays reachable in DR OSPFv3		
Condition:	DR Other Router goes down/disabled		
Workaround:	Wait for MaxAge to remove dead router's LSAs		

Defect ID:	DEFECT000660494		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.2.00	**Technology:**	CLI - Command Line Interface
Symptom:	Route map applied through BVM on MLXe is shown as successful even though it fails on device as below:- "ERROR: Please remove existing l2 routemap xyz first on port 3/1		
Condition:	Applying another route-map to an interface through BVM without removing the existing route-map		

Defect ID:	DEFECT000660530		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.2.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	LAG creation through BVM shows successful even though it is failed in device		
Condition:	LAG creation through BVM with participating ports do not have similar properties		

Defect ID:	DEFECT000660592		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	Static Routing (IPv4)
Symptom:	CPU may go High with the following ITC Queue full messages:- dest app id = 0x0000000c : src app id = 0x00000014 : msg type = 0x00140002 : error = ITC_ERR_DEST_QUEUE_FULL		
Condition:	12k IPv4 or IPv6 static routes		

Defect ID:	DEFECT000660604		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.2.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	Link may stay Up even though it is disabled in CLI		
Condition:	"loop back system" configured on the disabled port		
Workaround:	Loop back system should be configured on enabled port		

Defect ID:	DEFECT000661006		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 05.8.00	**Technology:**	IPv6 over MPLS VPN
Symptom:	IPv6 ping over vrf for remote BGP prefixes may not work on loopback interfaces		
Condition:	IPV6 prefixes learnt on user-vrf loopback interface through BGP over MPLS		

Defect ID:	DEFECT000661318		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP Route Reflector does not reflect VPNv4 or VPNv6 routes to reflector clients		
Condition:	1. Routes should be learned in BGP Route Reflector for address family VPNv4 or VPNv6 2. Execute 'clear ip bgp vpnv4 neighbor <neighbor-ip> soft-outbound' in BGP Route Reflector		
Recovery:	'clear ip bgp neighbor <neighbor-ip>' in BGP Route Reflector		

Defect ID:	DEFECT000661401		
Technical Severity:	High	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	OSPFv3 and IPV6 neighborship not formed with remote VPLS peer		
Condition:	Remote vpls peer configured with IPv6 on OSPFv3 interface with MPLS ttl policy applied		
Workaround:	Either of the following can be applied 1. Remove the commands `vrf-propagate-ttl and label-propagate-ttl enabled? under 'router mpls' configurations or 2. Configure static ipv6 neighbors		

Defect ID:	DEFECT000661413		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.6.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	CES/CER device may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20069c74: update_nh_hw_resource(pc) 20069b24: update_nh_hw_resource(lr) 20069fd8: write_nh_hw_entry 200731c0: update_nh_hw_entry 20069348: update_next_hop_entry 2006b0d0: update_backlink_table 2006b80c: mark_route_info_changed 2048dc58: lp_cam_update_arp_entry_pram 205bb284: process_one_arp_update_lp 20591dd0: process_one_arp_update 205920ec: process_arp_dy_messages 2034b01c: process_dy_change_packet 2037facc: ipc_multi_module_handler 2038222c: ipc_process_messages 203829ec: ipc_receive_packet 2037d308: ge_process_ipc_data_msg 2037d690: ge_process_ipc_msg 200b962c: metro_sys_loop 200af638: main 00040158: sys_end_task		
Condition:	Very rarely occurs with CER is configured as one of the BGP Speaker and processing ARP update messages		

Defect ID:	DEFECT000661452		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.2.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP routes learnt on Route Reflector for some of the existing clients might get lost		
Condition:	New route reflector client is added to the existing clients within the same VRF		
Recovery:	Recovered by any one of the following steps:- 1.'Clear ip bgp vpnv4 neighbor all soft in' 2. 'Clear ip bgp vpnv4 neighbor all soft' 3. Forcing each and every Route Reflector client to resend BGP updates		

Defect ID:	DEFECT000661617		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Active Management module may unexpectedly reload with the following stack trace:- 20ff077c: ospf_find_neighbor_from_grace_lsa(pc) 2104293c: age_the_link_state_database_entry(lr) 2104293c: age_the_link_state_database_entry 21041e0c: ospf_process_age_lsdb_entry 21041144: ospf_router_timer 2100a244: ospf_timer_callback 20b16280: itc_process_msgs_internal 20b16720: itc_process_msgs 2100a5b8: ospf_task 00005e18: sys_end_task		
Condition:	Occurs very rarely when the OSPF process is restarted from a problematic neighboring device to recover		

Defect ID:	DEFECT000661713		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.2.00	**Technology:**	IPv6 Addressing
Symptom:	Line card module may reload unexpectedly with the following stack trace:- 20a1cc64: ppcr_tx_packet(pc) 20a1d658: ppcr_tx_held_packet(lr) 20a1d658: ppcr_tx_held_packet 20fd8ce4: nd6_forward_ppcr_pending_pkt 20fd940c: nd6_process_all_pending_packets 20fd7a40: nd6_delete_neighbor_entry_from_cache 20fbc928: nd6_slave_incomplete_nei_aging_handler 20fbcad4: nd6_slave_incomplete_nei_aging 20fbc9b4: nd6_slave_timer 20fb90b8: ipv6_slave_timer 20005a74: perform_callback 2000647c: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f1664: main 00040158: sys_end_task		
Condition:	Very rarely occurs with large number of incomplete ND6 (IPv6 neighbor discovery) entries		

Defect ID:	DEFECT000661716		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 05.8.00	**Technology:**	sFlow
Symptom:	Extended MPLS VC data and Switch data's outgoing 802.1q VLAN may not be observed in SFLOW forwarded packets		
Condition:	SFLOW enabled for VPLS local switched packets		

Defect ID:	DEFECT000661722		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.0.00	**Technology:**	IPsec - IP Security
Symptom:	User may observe that IPSEC tunnel goes down and doesn't recover to up state		
Condition:	User may observe this on a system with scaled IPSEC configuration		

Defect ID:	DEFECT000661730		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 05.8.00	**Technology:**	NTP - Network Time Protocol
Symptom:	MLX, CES/CER may display incorrect Daylight/Summer time		
Condition:	for Australia (GMT+10) and New Zealand (GMT+12) time zones		

Defect ID:	DEFECT000661859		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.3.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	For LACP based LAG deployment, user might observe that the device connected to NI device is not showing LAG member interface in down/Blocked state while NI device interfaces are LACP-Blocked, when the peer is configured with different key id. To observe this behavior, two or more interfaces should be connected in a LAG topology between NI and peer device.		
Condition:	This is a mis-configuration scenario where user has two or more interfaces connected to NI device in a LAG topology and one of member interface is incorrectly configured with different LAG Key.		
Workaround:	To Avoid the behavior, user should configure same key on device connected to NI device.		
Recovery:	User should configure same key on device connected to NI device.and LACP Lag should recover from this situation.		

Defect ID:	DEFECT000661906		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 06.0.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Unexpected traffic loss in transit node with Class 0 Remap index updated as "54" instead of "0" in the following rate-limit output :- LP#dm rate-limit ppcr 0 0 : : Class Bound CIR CBS ACCRT EIR EBS ACERT Remap Remark ----- ----- --- --- ----- --- --- ----- ----- ------ 0 RX 5464064 10928128 10928128 5464064 10928128 10928128 '54' 0 0 TX 5464064 10928128 10928128 5464064 10928128 10928128 '54' 0		
Condition:	This is very rare scenario and happens on executing clear rate-limit counters multiple times when IP Receive ACL configured with Rate-limit policy in the router. ex : conf t policy-map rl-icmp cir 993568 cbs 2000000 end conf t ip receive access-list 192 sequence 30 policy-map rl-icmp end		

Defect ID:	DEFECT000661933		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.0.00	**Technology:**	ACLs - Access Control Lists
Symptom:	The command `ipv6 receive deactivate-acl-all? may not work sometimes		
Condition:	Observed after router reload		
Recovery:	Remove and reconfigure the command ?ipv6 receive deactivate-acl-all?		

Defect ID:	DEFECT000662137		
Technical Severity:	Medium	**Probability:**	Medium
Product:	NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.2.00	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Pim (*,G) entries formed in default vrf are also observed in non-default vrf mcache table		
Condition:	On executing the command `clear ip pim vrf <vrf-name> mcache?		

Defect ID:	DEFECT000662194		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.0.00	**Technology:**	Hardware Monitoring
Symptom:	'show optic <slot>' does not show any light levels		
Condition:	It is specific to Finisar QSFP28-CFP2 optic		

Defect ID:	DEFECT000662202		
Technical Severity:	Medium	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	CLI - Command Line Interface
Symptom:	'show chassis' displays power supply status as "Installed (Failed or Disconnected)" instead of "Installed (Shutdown)"		
Condition:	When 2100W power supply is manually powered off using command 'power-off power-supply #'		

Defect ID:	DEFECT000663193		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP static network routes might not get advertised to the peers		
Condition:	On Reload with BGP "static-network" routes configured Note: This may be observed from NI6.0 and higher releases only.		
Recovery:	Removing and adding back the static-network command		

Defect ID:	DEFECT000663296		
Technical Severity:	High	**Probability:**	Low
Product:	NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 06.0.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Traffic loss may be observed with Rate-limit policy		
Condition:	This is very rare scenario and happens on executing `clear rate-limit counters? multiple times when IP Receive ACL configured with Rate-limit policy. ex : conf t policy-map aaaaa cir xxxxxxx cbs yyyyyyy end conf t ip receive access-list zz sequence xy policy-map aaaaa end		

Closed without code changes NI6.3.00

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 08/30/2018 in NetIron OS 6.3.00.

Defect ID:	DEFECT000602148	**Technical Severity:**	Medium
Reason Code:	Not Reproducible	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.0.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	When Local CCEP goes DOWN and comes UP on MCT cluster device, BFD session with the MCT client devices can move to DOWN state and the session do not move to UP state again.		
Condition:	Condition: BFD configured on MCT cluster device for static routes. Trigger: When Local CCEP goes DOWN and comes UP again on MCT cluster device, this issue could occur.		
Recovery:	execute "clear bfd neighbors x.x.x.x" on the device where this issue is observed		

Defect ID:	DEFECT000644706	**Technical Severity:**	High
Reason Code:	Not Reproducible	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.0.00	**Technology:**	PIM6 - IPv6 Protocol-Independent Multicast
Symptom:	Customer can notice traffic loss for IPv6 multicast traffic.		
Condition:	When both IPv4 and IPv6 multicast traffic is running and IPv6 multicast routes are cleared using "clear ipv6 pim cache".		

Defect ID:	DEFECT000649337	**Technical Severity:**	High
Reason Code:	Not Reproducible	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.2.00	**Technology:**	IPv4 Multicast Routing
Symptom:	User may observe drop in the traffic which is getting forwarded on an IPSEC tunnel		
Condition:	This issue may be seen when failover happens for IPSEC tunnel		

Defect ID:	DEFECT000653077	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 05.8.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	BGP session may flap		
Condition:	SNMP polling of BGP tables (bgp4PathAttrTable, bgp4V2NlriTable) with 600K or more BGP route entries		
Workaround:	Disable SNMP polling for the table: bgp4PathAttrTable, bgp4V2NlriTable		

Defect ID:	DEFECT000654629	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 05.8.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	CCP protocol does not go down on MCT cluster node		
Condition:	1. MCT cluster with L2VPN peer should be configured on both the Cluster peer nodes 2. "client-interface shutdown" command should be issued on the MCT Active Cluster node		

Defect ID:	DEFECT000654631	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 05.8.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	"client-interface shutdown" command does not bring the CCP down and MCT VLL Active/Standby switchover does not happen		
Condition:	(1) MCT cluster with VPLS and VLL should be configured on both the peer nodes . (2)"client-interface shutdown" command should be issued on MCT Active cluster node		

Defect ID:	DEFECT000654707	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 05.8.00	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Line card may reload unexpectedly with the following stack trace:- 21584ddc: memcpy(pc) 20f48b28: pimsm_encapsulate_pkt_and_send_to_rp(lr) 20f4987c: pimsm_forward_multicast_pkt 20f4850c: pim_forward_multicast 20f27d98: mcast_flow_fast_forward 20eaeb3c: fpip_process_ip_packet_with_l2_broadcast 20eedb20: rx_pkt_processing 20d4f4a4: lp_pkt_receive 20a0f028: ppcr_recieve_packet 207eef3c: lp_pbif_packet_task 00040158: sys_end_task		
Condition:	Flap the interface on MCT Peer repeatedly with multicast-routing and PIM SM configured on MCT		

Defect ID:	DEFECT000654817	**Technical Severity:**	High
Reason Code:	Already Fixed in Release	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	CES/CER may unexpectedly reload with the following stack trace :- 205e15d8: time_tree_delete_first_entry_and_add(pc) 205e1de8: trace_util_add_entry_avl(lr) 205e1de8: trace_util_add_entry_avl 20598540: IPTRACE_AVL 20598294: IPTRACE_AVL_USING_RT_ENTRY 204cacd8: lp_cam_add_ip_nexthop_route 204ca61c: lp_cam_add_ip_route 205b0674: ip_update_pram_for_route_entry_puma 205b08ec: ip_update_pram_for_route_entry 206497bc: dp_trie_process_one_route_update 2064a124: dp_trie_process_route_update 2064a2bc: process_tree_dy_messages 203793cc: process_dy_change_packet 203ae898: ipc_multi_module_handler 203b0e74: ipc_process_messages 203b1634: ipc_receive_packet 203abef0: ge_process_ipc_data_msg 203ac278: ge_process_ipc_msg 200bb704: metro_sys_loop 200b10e0: main 00040158: sys_end_task		
Condition:	It is very rarely observed with the following scale on CES/CER MCT Cluster by flapping ICL interface repeatedly 250 VPLS instances 100 VLL 500 IGMP group 250 MLD group		

Defect ID:	DEFECT000655355	**Technical Severity:**	Medium
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.0.00	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Port of 20X10G Line card Module may not come up		
Condition:	It is very rarely observed when a new connection is made on a port of 20X10G		
Recovery:	Any one of the following methods can help in recovery:- 1. Removal and Re-insert of SFPP 2. Swap SFPP by SFP and re-swap SFP by SFPP. 3. Reload Line card Module.		

Defect ID:	DEFECT000658063	**Technical Severity:**	Medium
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 05.8.00	**Technology:**	ACLs - Access Control Lists
Symptom:	May observe the following syslog message:- Apr 2 00:33:12 Dut list 0 denied all 0.0.0.0(xyz)(Ethernet x/y 0000.0000.0000) -> 0.0.0.0(n), abc event(s)		
Condition:	Two ACL's with deny rule binded to the same interface with deny logging enabled		

Defect ID:	DEFECT000658976	**Technical Severity:**	Medium
Reason Code:	Already Fixed in Release	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 05.6.00	**Technology:**	Hardware Monitoring
Symptom:	Observed incorrect Timestamp in 'show tm log' output		
Condition:	On execution of ?show tm log?		

Defect ID:	DEFECT000659925	**Technical Severity:**	Medium
Reason Code:	Design Limitation	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.2.00	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD neighbor session would take 3 minutes to come up on bringing up the interface		
Condition:	(1) bring up the BFD session between the neighbors with the image below 5.7 or above loaded (2) bring DOWN the interface (3) bring UP the interface		

Known issues NI6.3.00

This section lists open software defects with Critical, High, and Medium Technical Severity as of 08/30/2018 in NetIron OS 6.3.00.

Defect ID:	DEFECT000605799		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.1.00	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Momentary traffic loss will be seen when device switch-over from active MP to standby MP.		
Condition:	During MP switch-over, hardware reprogramming of some of the existing multicast entries can cause momentary traffic loss.		

Defect ID:	DEFECT000622581		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.1.00	**Technology:**	PIM6 - IPv6 Protocol-Independent Multicast
Symptom:	After reload, traffic flow for some groups gets delayed until the PIM mcache is populated. This can take a maximum of 125s or the IGMP query interval time configured.		
Condition:	This can happen on the PIM router receiving the IGMP report when it is not the RP in the PIM network and IGMP reports are received before the RPF path towards the RP is available		

Defect ID:	DEFECT000623241		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.1.00	**Technology:**	NTP - Network Time Protocol
Symptom:	CES/CER does not synchronize time with NTP broadcast server.		
Condition:	NTP broadcast client configuration on default or non default VRF.		

Defect ID:	DEFECT000623781		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 05.9.00	**Technology:**	ACLs - Access Control Lists
Symptom:	ingress packets could be dropped when allow-all-vlan pbr is configured		
Condition:	ingress packets could be dropped when allow-all-vlan pbr is configured on a 4x40 module.		

Defect ID:	DEFECT000631492		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.0.00	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	(*, G) and (S, G) entries may not be removed from IGMP snooping VLAN database		
Condition:	IGMP leave message received from the last receiver port		

Defect ID:	DEFECT000632633		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.0.00	**Technology:**	PIM6 - IPv6 Protocol-Independent Multicast
Symptom:	IPv6 multicast traffic dropped on scaled system		
Condition:	The cam profiling is configured as "multi-service-6" Card type is NI-MLX-10Gx8-M IPV6 multicast CAM size is allocated more than 4k		

Defect ID:	DEFECT000633774		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Standby Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20ec94d4: bgp_check_for_fwd_address(pc) 20ec93ec: bgp_check_for_fwd_address(lr) 20efbd18: bgp_RIB_in_delete_route 20f7952c: bgp_check_for_aggrgation 20effd40: bgp_remove_route_advertisement 20efbdf4: bgp_RIB_in_delete_route 20efda08: bgp_vrf_RIB_in_delete_all_self_nlris 20eb4e88: bgp_clear_all_vrf_neighbors 20f57744: bgp_clear_neighbor_itc_request_callback 20b14584: itc_process_msgs_internal 20b14a24: itc_process_msgs 20f73ed8: bgp_task 00005e18: sys_end_task		
Condition:	Execution of "clear ip bgp neighbor all" command		

Defect ID:	DEFECT000636007		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 05.8.00	**Technology:**	CLI - Command Line Interface
Symptom:	InOctet and OutOctet counter values do not include the Ethernet framing overhead bytes.		
Condition:	When executing ?show statistics? command after enabling include-ethernet-framing-overhead configuration command. OR When polling the below SNMP OID?s after enabling include-ethernet-framing-overhead configuration command. ? ifInOctets ? ifOutOctets ? ifHCInOctets ? ifHCOutOctets ? snSwIfInOctets ? snSwIfOutOctets.		

Defect ID:	DEFECT000638634		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 05.8.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	The LAG port may not go down on receiving the timed-out LACP BPDU from peer with reset of collecting and distributing bits		
Condition:	Mac access-list with explicit deny all is configured on a LAG port		

Defect ID:	DEFECT000642613		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.6.00	**Technology:**	VRRPv3 - Virtual Router Redundancy Protocol Version 3
Symptom:	High CPU usage causing dual master VRRP and VRRPv3 dual master .		
Condition:	Number of ND6 entries is greater than 12000 on CES/CER		

Defect ID:	DEFECT000643261		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.0.00	**Technology:**	IPv4 Multicast VLAN Traffic Reduction
Symptom:	A host receives multicast traffic for an IGMP group for which it has not sent an IGMP JOIN message.		
Condition:	A PC Host receives multicast traffic, even if it has not sent an IGMP Join message for the multicast group. Conditions: a. An active receiver on one of the ports of vlan.(with IGMP snooping enabled). Other ports of vlan do not receive multicast traffic. b. Disable IGMP snooping on the vlan. MC traffic resumes(due to default flooding behavior on vlan). c. Re-enable the IGMP snooping configuration. d. All the ports of vlan continue to receive the multicast traffic.		

Defect ID:	DEFECT000643881		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Inconsistent behavior may be observed between OSPFV2 and OSPFV3		
Condition:	Configuration of 'max-metric' command		

Defect ID:	DEFECT000652797		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.2.00	**Technology:**	sFlow
Symptom:	When sFlow is enabled for IPV6 traffic sampling on an interface which is associated with a VE and user defined VRF, the LP CPU usage may go high up to 50%.		
Condition:	When sFlow is enabled on an interface which is associated with a VE and user defined VRF and IPV6 traffic is sampled whose destination is 1+ hops away, the LP CPU usage (for the LP where sampling is taking place) could be considerably high (about 7 times) compared to when the interface is not associated with a VE.		
Workaround:	LP CPU usage can be reduced by either reducing the sampling frequency (via increasing the 'sampling rate' configuration) or by removing the VE configuration on sFlow forwarding port.		
Recovery:	Disable sFlow, reconfigure as needed and re-enable sFlow.		

Defect ID:	DEFECT000656284		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 05.8.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Rate limit traffic drops may not be observed on the configured port		
Condition:	On execution of `clear rate-limit counters?		
Workaround:	Reload the line card		

Defect ID:	DEFECT000657027		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.2.00	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	(S,G) for some groups are not formed in intermediate CER router		
Condition:	Rarely observed with PIM-DM enabled on all the interfaces during router upgrade		

Defect ID:	DEFECT000657175		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.2.00	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Multicast traffic drops in a multicast snooping enabled switch which is directly connected to Source		
Condition:	Rarely observed on a Multicast snooping enabled switch configured with multicast passive on VLAN		

Defect ID:	DEFECT000657277		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	SDN
Reported In Release:	NI 05.8.00	**Technology:**	OpenFlow
Symptom:	Sometimes Open flow rules may not get installed		
Condition:	On receiving the update action within a second, while processing the same Open flow rule with same priority and priority should be less that the existing flow		

Defect ID:	DEFECT000657631		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.2.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	VPLS traffic may be dropped on the MCT peer node		
Condition:	1) MCT over VPLS should be configured 2) 'Client interface shutdown' has to be configured on VPLS active node to make the CCEP port disable 3) After traffic switched to the MCT peer node which is the new active node, reload the current passive MCT VPLS node		

Defect ID:	DEFECT000658979		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 06.0.00	**Technology:**	MPLS Traffic Engineering
Symptom:	LSP session may not go down		
Condition:	1) MPLS LSP tunnel should be established with the remote peer 2) Disable the loop back interface (peer IP) on the remote device		

Defect ID:	DEFECT000659209		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Multicast
Reported In Release:	NI 06.0.00	**Technology:**	IPv4 Multicast Routing
Symptom:	Multicast traffic may drop in PIM router below RP which is connected towards the receiver in non-default VRF		
Condition:	Rarely observed after PIM RP node reloads		
Workaround:	Execute clear ip pim mcache vrf <vrf-name> in downstream router after RP		

Defect ID:	DEFECT000659554		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.0.00	**Technology:**	CLI - Command Line Interface
Symptom:	'fan-threshold' configuration is not saved in running-configuration after reload		
Condition:	Fan speed is manually configured using 'fan-threshold' command		

Defect ID:	DEFECT000661201		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Ipv6 BGP peering session may encounter "Optional attribute error"		
Condition:	1. IPv6 Additional-Paths option is enabled 2. Processed withdraw message from neighbor		

Defect ID:	DEFECT000661407		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	IPv6 traffic may not be forwarded over VEoVPLS interface		
Condition:	MPLS LSP primary path goes down on disabling the VEoVPLS interface		
Workaround:	clear mpls lsp <lsp-name>		

Defect ID:	DEFECT000661679		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Management
Reported In Release:	NI 06.2.00	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	ifPhysAddress may return primary port physical MAC address		
Condition:	for all the member ports other than primary port in a LAG		

Defect ID:	DEFECT000661865		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	ICMP - Internet Control Message Protocol
Symptom:	IPv6 traffic may not be forwarded to destined port		
Condition:	Specific to Ipv6 Hop-by-hop and fragmented packets		
Workaround:	Frequency of this issue can be lowered by configuring maximum value in the below configuration command "ipv6 nd reachable-time <secs>"		

Defect ID:	DEFECT000662001		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Security
Reported In Release:	NI 06.2.00	**Technology:**	ACLs - Access Control Lists
Symptom:	Traffic loss with TX ACL drops may be observed in 'show np stat'		
Condition:	1) Ingress port has to be configured with PBR route-map with flood vlan 2)Transparent vlan flooding has to be enabled on the egress vlan 3)Egress port should be 40G and configured with loopback system		

Defect ID:	DEFECT000662025		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	MPLS
Reported In Release:	NI 06.0.00	**Technology:**	MPLS Traffic Engineering
Symptom:	FRR Facility backup LSP is not up		
Condition:	When "ip ospf passive" is configured on interface, there is no notification sent to MPLS deamon to cause TE flush or rsvp igp sync reaction.		

Defect ID:	DEFECT000662210		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.0.00	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	BGP multipaths are not happened properly for BGP IPv6 routes that are learned in VRF		
Condition:	1. iBGP neigborship established with 2 neighbors in VRF 2. BGP multipaths are enabled 3. The same route is advertised from both the neighbors with the same local_pref, MED, ORIGIN, weight		
Workaround:	Configure "always-compare-med" in 'router bgp'		

Defect ID:	DEFECT000662260		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Traffic Management
Reported In Release:	NI 06.2.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Burst traffic may be forwarded more than the configured rate on CES/CER		
Condition:	Bursty traffic with Rate-limit is configured on the interface		

Defect ID:	DEFECT000662321		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 05.8.00	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	High CPU may be observed on CER		
Condition:	Processed high rate of fragmented DHCP protocol packets		

Defect ID:	DEFECT000662992		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.3.00	**Technology:**	IS-IS - IPv4 Intermediate System to Intermediate System
Symptom:	User may observe reload of standby MP		
Condition:	User may observe this issue on a system with scaled IS-IS configuration when "clear isis all" is issued		

Defect ID:	DEFECT000664218		
Technical Severity:	Low	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	Monitoring
Reported In Release:	NI 06.2.00	**Technology:**	Syslog
Symptom:	telnet client may not be observed in 'show logging' as configured		
Condition:	'telnet client <ip-address>' is configured from a telnet session.		

Defect ID:	DEFECT000664742		
Technical Severity:	High	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.3.00	**Technology:**	IS-IS - IPv4 Intermediate System to Intermediate System
Symptom:	User may observe that IS-IS routes are not advertised to the neighbors		
Condition:	User may observe this issue on a system with scaled IS-IS configuration and many loopback interfaces.		
Recovery:	User can issue "clear isis all" on the system that is not advertising IS-IS routes to the neighbors		

Defect ID:	DEFECT000665208		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	NI 06.0.00	**Technology:**	VLAN - Virtual LAN
Symptom:	Sometimes SSH session may not respond		
Condition:	1. Pasting large configuration list of commands around 20K lines 2. Another session is opened for the same device		

Defect ID:	DEFECT000665302		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	NI 06.3.00	**Technology:**	Multi-VRF
Symptom:	Route for loopback interfaces might not be advertised to BGP peers after a router reload.		
Condition:	With a BGP configuration over 100 BGP VRFs and a large configuration file		
Recovery:	a. disable/enable the loopback interfaces, or b. clear ip bgp neighbor all soft out, or c. clear ip bgp local routes		