21 March 2019

NI OS 06.1.00a for ExtremeRouting MLX Series Devices

Release Notes 4.0

9036124-00

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial release	03/24/2017
2.0	Updated supported modules table.	10/19/2017
3.0	Updated unsupported modules table	10/20/2017
4.0	Replaced section “Unsupported, End of Life Hardware” with section “End of Sale and End of Support products”.	03/21/2019

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 06.1.00 introduces new functionalities and enhances the capabilities of ExtremeRouting MLX Series, ExtremeRouting CER 2000 Series and ExtremeSwitching CES 2000 Series. Extreme continues to innovate in key technologies and Release 06.1.00 brings new features in the following areas:

* SDN,

* Data privacy with IPsec,

* Routing and MPLS services,

* Network Packet Broker functionality for 4G/LTE mobile networks

This release will provide customers the capability to load-balance OpenFlow traffic across multiple MPLS LSPs in their network.

OpenFlow traffic can now be mapped to IPSEC tunnels so customers have fine grained control over the traffic they want to secure over the internet or other unsecured networks with NI 06.1.00.

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

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

Behavior changes

Behavior changes in release NI 06.1.00

SNMP default community

The default SNMP public community “ro” will no longer work with NI 6.1 as it was removed due to a security threat arising from not explicitly configuring a community. Going forward the user will have to explicitly configure a community in NI devices to perform SNMP operations.

“hd” (Hex Dump) command has been deprecated in R06.1.00

For other behavior changes, consult the Software Features, the CLI Command, and the Upgrade and Downgrade Considerations sections of these notes for any behavior changes in this release.

There are no deprecated commands in R06.1.00a.

Software Features

New software features introduced in R06.1.00a

No new software features introduced in release R06.1.00a.

New software features

The following software features are new in this release. For information about which platforms support these features, refer to the Feature Support Matrix.

IP Routing, forwarding, MPLS features

- **Source IP of LDP session**: Customer can now configure the interface address as source (and transport) address of LDP sessions with this feature thus providing better security in their network
- **NTP in management VRF**: This feature allows restricting NTP control packets to management VRF alone which was not possible in the prior releases
- **IPv4/IPv6 PIM scalability for MCT to 8000**: Enhancement of multicast caching entries for PIM over MCT from 2000 to 8000 (S,G) entries
- **IPv6 PBR with MPLS, GRE as nexthop**: This feature allows customers to transport IPv6 traffic over IPv4 islands with either MPLS or GRE as tunnel encapsulation
- **IPv6 ACL rate-limiting**: Prior to this release CES/CER only supported L2 and IPv4 ACL rate-limiting. This release enhances support for IPv6 as well on the CES/CER platforms. The feature also allows doing the rate-limiting on non-default VRFs
- **Traffic classification based on MPLS EXP**: With this feature traffic class value is based on the received EXP value of the MPLS header to enable correct queueing
- **IPv6 ACL group scale increase to 4000**: Prior to this release MLX supported 4000 IPv4 ACLs, this feature increases support for IPv6 ACLs to 4000 as well

Software Defined Networking

- **OpenFlow traffic load-balancing across MPLS LSPs**: With this feature customers will be able to load-balance OpenFlow traffic across multiple LSPs. Group table type SELECT is implemented in this release to support this capability

- **PBR/ACL and OF on the same port**: Customers can now enable PBR and ACL on the same port that OpenFlow is enabled in. Depending on the PBR configuration traffic will undergo both OpenFlow and PBR processing

- **Untagged matching support in OF**: Prior to this release OpenFlow matching rules did not support untagged traffic. This feature enables this capability

- There is a feature addition in this release that allows setting per-slot np-openflow-flow-entries system-max without requiring a chassis reload:

IPSEC

- **OpenFlow to IPSEC logical port**: This feature allows OpenFlow matching traffic to be mapped to IPSEC tunnels. Traffic can also be load-balanced across multiple IPSEC tunnels. Same group table type SELECT that is used for LSP balancing is employed for IPSEC tunnel load-balancing as well

Network Packet Broker

- **GTP de-encapsulation**: Outer-IP, outer-UDP header and the GTP header of GTP-U packets ingressing the system can now be removed to retain the MAC and inner L3 and L4 headers only with this new feature

- **VXLAN header stripping**: This feature helps strip the outer L2, L3, L4 VXLAN headers from the incoming VXLAN packets to be able to process the customer frame

Management and RAS feature enhancements

- **Saving system information to flash**: This feature collects and saves system (both MM and LC) information for debugging purposes at the customer site

- **Management IP as SNMP trap-source**: Management IP address can be set as the trap-source IP via the 'snmp-server trap-source' command with this feature

- **SCP based simplified upgrade**: In addition to simplified upgrade supported using package located at TFTP server SCP is used to copy files to the device compact flash using SCP server function in the device. A linux python script is provided to enable this copying and upgrading tasks using SCP

- **Firmware integrity check**: This feature implements doing an integrity check after SCP download of firmware to ensure the downloaded code is the same as in the source location

- **Optical monitoring MIB enhancement**: This feature will allow obtaining optics TX and RX power status and power values (in units of microwatt). Existing Optical Lane Monitoring MIB tables have been enhanced with two new tables to provide these values.

- **Data collection from the LP**: Errors in MP to LP communication can now be logged in the LP console or to syslog with this feature

- **System-wide flow control status**: This feature helps identifying and troubleshooting network traffic performance and drop issues because of flow control conditions in the system. CLI commands are introduced with this feature to display flow control status at the MAC port, NP, and TM levels. Commands are available at MP and NP to get this information

New Optics support

- CWDM4 (QSFP28) 100G optics support is added in this release

Other enhancements

- This release fixes incorrect destination MAC in sFlow for L3 traffic

- This release fixes incorrect out IP length in GRE after truncating packet

CLI commands

New CLI commands R06.1.00a

No new commands were introduced in release R06.1.00a.

CLI commands introduced

New CLI commands R06.1.00

The following commands are new in this release:

- gtp-de-encapsulation – new command to remove GTP header
- strip-vxlan – new command to strip VxLAN header
- tunnel mode ipsec openflow-hybrid – enables openflow-hybrid on an IPSec tunnel
- memdump slot <slot_id> - this command dumps system info for a slot into memory
- show gtp-de-encapsulation
- ip multicast-routing optimization mct-scaling – enabled multicast scaling optimization for MCT
- ipv6 multicast-routing optimization mct-scaling - enabled multicast scaling optimization for MCT
- enable firmware-integrity-check - This command enables the RSA2048 key and SHA256 hash digital signature based firmware integrity check when the image is downloaded and installed on the device.
- verify { md5|sha1|sha256 } file <filenm> [<hex_digest> | {digest-file <filenm>}] – this command verifies the encryption hash of a file
- verify signature file <filenm> signature-file <filenm> - this command can be used to verify the signature of a file
- Show ip igmp cluster-client group- this command displays the cluster client group on MCT peers for ipv4.
- Show ipv6 mld cluster-client group- this command displays the cluster client group on MCT peers for ipv6
- debug ip igmp mct-mdup- this command shows debug for the igmp group synced between MCT peers
- debug ipv6 mld mct-mdup- this command shows debug for the igmp group synced between MCT peers

Modified commands

The following commands have been modified for this release:

- openflow enable ofv130 acl_pbr – existing command extended to allow enable/disable of ACL/PBR globally
- snmp-server trap-source management – new option ‘management’ introduced to allow configuration of management IP address as trap source
- management-vrf command under ‘config ntp’ context – this allows enable/disable of NTP on a management VRF

- extended-qos-mode set-force-tc-match-label-exp - to enable force the traffic class by new CLI command “set-force-tc-match-label-exp”. This command will be allowed with presence of “extended-qos-mode”
- set next-hop-ip-tunnel – this command was only supported for IPv4 PBR. With the introduction of IPv6 PBR with GRE tunnel as next hop, this command is now allowed for IPv6 PBR
- set next-hop-lsp lsp-name - this command was only supported for IPv4 PBR. With the introduction of IPv6 PBR with MPLS tunnel as next hop, this command is now allowed for IPv6 PBR
- rate-limit – this command on CES/CER has been extended to accept IPv6 ACL to allow IPv6 rate limiting ACLs
- rate-limit – this command has been extended on CES/CER to accept “vrf” name to enable rate limiting on a particular VRF
- set next-hop-tvf-domain <tvf-domain-id> replace-vlan <vlan-X> - “replace-vlan” is newly introduced
- set next-hop-flood-vlan <vlan-id> replace-vlan <vlan-X> - “replace-vlan” is newly introduced
- transport-address interface – this command is newly introduced under MPLS interface’s “lsp-params” CLI context to set transport address for LDP
- reload -x – reload system after memory dump
- reset -x – reset LP after memory dump
    - show interface – displays GTP de-encapsulation status
    - show packet-encap-processing – displays the configuration state of VxLAN header including others
    - show openflow - this command output includes information about logical interface (MPLS and IPSec tunnels)
    - show openflow flow – this command displays flows including vlan modification configurations
    - show openflow group – this command is enhanced to include information about groups with logical interfaces
    - show openflow interface - this command is enhanced to display enabled logical Interface (MPLS and IPSec) information
    - show ipsec interface – this command output extended to display openflow status (enabled/disabled) on IPSec tunnel
    - show route-map – Output includes additional information about replace-vlan
    - show tvf-domain – Output includes additional information about replace-vlan
- show openflow – command output modified to include status of ACL/PBR
- radius-server host – Existing CLI extended to accept IPv6 address to support IPv6 Authentication/accounting for RADIUS over TLS and configurable shared-key along with the server
- show management-vrf – the output of this command is extended to display the statistics of NTP packets/sessions rejection due to failure in Management vrf validation
- show tsec — some counters in the display output are no longer clear on read, hence “Total” keyword has been inserted to reflect that
- show optics — Tx and Rx power value of optics is displayed in units of Micro Watts (uW) along with existing dBm values
- show optics threshold — Tx and Rx power value of optics is displayed in units of Micro Watts (uW) along with existing dBm values

- show mpls ldp interface - this command is modified to show if LDP interface transport address feature is in use
- show mpls ldp sess - this command is modified to show which interface transport address is in use
- show flow-ctrl status – command extended to display RX Pause status for ports
- show ip pim count mct – displays various scaling related PIM/MCT counters
- show ipv6 pim count mct – displays various scaling related PIM/MCT counters
- Show ip pim global- this command displays information about MCT scaling optimization is enabled
- Show ipv6 pim global- this command displays information about MCT scaling optimization is enabled

Deprecated commands

The following commands have been deprecated beginning with this release:

- hd – hex dump command has been removed from system

MIBs and messages

MIBs

New MIB Objects

No MIB objects were introduced in release R06.1.00a.

New MIB Objects

The following MIBs are introduced in release R06.1.00:

- Following is a newly added table snIfOpticalMonitoring2Table, which is augmented from the existing table snIfOpticalMonitoringInfoTable for displaying one of the following status values: notSupported(1), notApplicable(2), highAlarm(3), highWarn(4), normal(5), lowWarn(6), lowAlarm(7) and the Tx Power and Rx Power value in units of microwatt.

snIfOpticalMonitoring2Table – new OID (1.3.6.1.4.1.1991.1.1.3.3.12)

- snIfOpticalMonitoring2TxPowerStatus
- snIfOpticalMonitoring2TxPowerVal
- snIfOpticalMonitoring2RxPowerStatus
- snIfOpticalMonitoring2RxPowerVal

- Following is a newly added table snIfOpticalLaneMonitoring2Table, which is augmented from the existing table snIfOpticalLaneMonitoringTable for displaying one of the following status values: notSupported(1), notApplicable(2), highAlarm(3), highWarn(4), normal(5), lowWarn(6), lowAlarm(7) and the Tx Power and Rx Power value in units of microwatt.

snIfOpticalLaneMonitoring2Table – new OID (.1.3.6.1.4.1.1991.1.1.3.3.13)

snIfOpticalLaneMonitoring2TxPowerStatus
snIfOpticalLaneMonitoring2TxPowerVal
snIfOpticalLaneMonitoring2RxPowerStatus
snIfOpticalLaneMonitoring2RxPowerVal

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

No new RFCs are supported in this release.

Hardware support

Supported devices

The following devices are supported in this release:

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

Supported devices for Network Packet Broker R06.1.00

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-100GX1-X	MLX Series 1-port 100 GbE module with IPv4/IPv6/MPLS hardware support—requires high-speed switch fabric modules and CFP optics.	Yes	Yes	2
BR-MLX-100GX2-X	MLX Series 2-port 100 GbE module with IPv4/IPv6/MPLS hardware support—requires high-speed switch fabric modules and CFP optics.	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 NetIron XMR/MLX AC
NI-X-DCPWR-A	1200W power supply.	4-Slot NetIron XMR/MLX DC

BR-MLXE-32-ACPWR-3000	AC 3000W power supply.	32-slot NetIron MLXe/XMR/MLX
BR-MLXE-32-DCPWR-3000	DC 3000W power supply.	32-slot NetIron MLXe/XMR/MLX
NIBI-32-ACPWR-A	AC 2400W power supply.	32-Slot NetIron MLXe/XMR/MLX
NIBI-32-DCPWR	2400W power supply.	32-Slot NetIron 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.

The NetIron 06.1.00 release includes support for the following:

Item	Description
100G-QSFP28-CWDM4-2KM	100GBASE CWDM4 QSFP TRANS LC 2KM OVER SM
100G-QSFP28-LR4-10KM	100GBE QSFP28 (LC),LR4,10 KM OVER SMF
10G-SFPP-SR	10GBASE-SR,SFP+ OPTIC (LC),300M MMF
10G-SFPP-ER	10GBASE-ER, SFP+ OPTIC (LC),UP TO 40KM

End of Sale and End of Support products

For more information on product support, refer to the End of Sale and End of Support page.

Software upgrade and downgrade

Image file names

Download the following images from www.extremenetworks.com.

MLX Series and NetIron XMR devices

NOTE: When upgrading Multi-Service Ironware for MLX Series/XMR, 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 R06.1.00a MLX Series/XMR software upgrade

```
# Manifest File for XMR/MLX Release 06.1.00

-NETIRON_IRONWARE_VER XMR-MLXV6.1.00a
#=================================================================

-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin

-DIRECTORY /Boot/ManagementModule
xmprm05900.bin

#  Application Images
-DIRECTORY /Combined/FPGA
lpfpga06100a.bin

-DIRECTORY /Combined/Application
xm06100a.bin

-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin

-DIRECTORY /Monitor/ManagementModule
xmb06000.bin

-DIRECTORY /Application/ManagementModule
xmr06100a.bin

-DIRECTORY /Application/InterfaceModule
xmlp06100a.bin

-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06100a.bin 2.11
pbif8x10_06100a.bin 2.24
pbifmrj_06100a.bin 4.04
pbifsp2_06100a.bin 4.02
statsmrj_06100a.bin 0.09
```

```
xgmacsp2_06100a.bin 0.17
xpp2x100_06100a.bin 1.05
xpp4x40_06100a.bin 6.10
xpp4x10g3_06100a.bin 5.00
xpp8x10_06100a.bin 1.08
xppmrj_06100a.bin 1.03
xppsp2_06100a.bin 1.01
xppxsp2_06100a.bin 1.01
pbif-ber-g3_06100a.bin 2.11
xpp20x10g3_06100a.bin 7.00
xpp2x100g3_06100a.bin 7.00

-DIRECTORY /FPGA/ManagementModule
mbridge32_06100a.xsvf 36
mbridge_06100a.xsvf 37
sbridge_06100a.mcs 6
hsbridge_06100a.mcs 17

-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06000.sig
xmb06000.sig
xmr06100a.sig
xmlp06100a.sig
lpfpga06100a.sig
hsbridge_06100a.sig
mbridge_06100a.sig
mbridge32_06100a.sig
sbridge_06100a.sig
pbif4x40_06100a.sig
pbif8x10_06100a.sig
pbifmrj_06100a.sig
pbifsp2_06100a.sig
pbif-ber-g3_06100a.sig
statsmrj_06100a.sig
xgmacsp2_06100a.sig
xpp2x100_06100a.sig
xpp20x10g3_06100a.sig
xpp2x100g3_06100a.sig
xpp4x40_06100a.sig
xpp4x10g3_06100a.sig
xpp8x10_06100a.sig
xppmrj_06100a.sig
xppsp2_06100a.sig
xppxsp2_06100a.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
```

```
xmr06100a.sha256
xmlp06100a.sha256
lpfpga06100a.sha256
hsbridge_06100a.sha256
mbridge_06100a.sha256
mbridge32_06100a.sha256
sbridge_06100a.sha256
pbif4x40_06100a.sha256
pbif8x10_06100a.sha256
pbifmrj_06100a.sha256
pbifsp2_06100a.sha256
pbif-ber-g3_06100a.sha256
statsmrj_06100a.sha256
xgmacsp2_06100a.sha256
xpp2x100_06100a.sha256
xpp20x10g3_06100a.sha256
xpp2x100g3_06100a.sha256
xpp4x40_06100a.sha256
xpp4x10g3_06100a.sha256
xpp8x10_06100a.sha256
xppmrj_06100a.sha256
xppsp2_06100a.sha256
xppxsp2_06100a.sha256

#  MIBS:

-DIRECTORY /MIBS
xmr06100a.mib
xmr06100a_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

MLX06100a_mnf.txt
MLX06100a_mnf.sig
MLX06100a_mnf.sha256
```

FPGA file names and supported modules

File Name	Supported Modules
pbif4x40_06100.bin	4x40G modules
pbif8x10_06100.bin	8x10G modules
pbifmrj_06100.bin	24x1G and 48x1G modules
pbifsp2_06100.bin	2x10G, 4x10G, 4x10G-x and 20x1G modules
statsmrj_06100.bin	24x1G and 48x1G modules
xgmacsp2_06100.bin	2x10G, 4x10G-x and 4x10G modules
xpp2x100_06100.bin	2x100G modules (double-wide CFP-based module)
xpp4x40_06100.bin	4x40G modules
xpp4x10g3_06100.bin	4x10G modules
xpp8x10_06100.bin	8x10G modules
xppmrj_06100.bin	24x1G and 48x1G modules
xppsp2_06100.bin	2x10G, 4x10G, and 20x1G modules
xppxsp2_06100.bin	4x10G-x
pbif-ber-g3_06100.bin	20x10G and 2x100G modules (-M and –X2)
xpp20x10g3_06100.bin	20x10G modules
xpp2x100g3_06100.bin	2x100G modules (half-slot CFP2-based module)
mbridge32_06100.xsvf	MBRIDGE32
mbridge_06100.xsvf	MBRIDGE
sbridge_06100.mcs	Switch fabric modules
hsbridge_06100.mcs	High speed switch fabric modules

NetIron CES and NetIron CER devices

When upgrading Multi-Service Ironware for CES/CER, 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.

```
-NETIRON_IRONWARE_VER CES-CERV6.1.00a

#====================================================================
-DIRECTORY /Boot
ceb06000.bin

-DIRECTORY /Application
ce06100a.bin

-DIRECTORY /FPGA
pbifmetro_06100a.bin
```

```
-END_OF_IMAGES

-DIRECTORY /Signatures
ceb06000.sig
ce06100a.sig
pbifmetro_06100a.sig
ceb06000.sha256
ce06100a.sha256
pbifmetro_06100a.sha256

-DIRECTORY /MIBS
ce06100a.mib
ce06100a_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-CER06100a_mnf.txt
CES-CER06100a_mnf.sig
CES-CER06100a_mnf.sha256

-DIRECTORY /Manuals
```

Manifest for Network Packet Broker devices

NOTE: When upgrading Multi-Service Ironware for MLX Series/XMR, 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 R06.1.00a software upgrade

```
# Manifest File for XMR/MLX Release 06.1.00

-NETIRON_IRONWARE_VER XMR-MLXV6.1.00a
#====================================================================
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin

-DIRECTORY /Boot/ManagementModule
xmprm05900.bin
```

```
# Application Images
-DIRECTORY /Combined/FPGA
lpfpga_npb_06100a.bin

-DIRECTORY /Combined/Application
xm06100a.bin

-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin

-DIRECTORY /Monitor/ManagementModule
xmb06000.bin

-DIRECTORY /Application/ManagementModule
xmr06100a.bin

-DIRECTORY /Application/InterfaceModule
xmlp06100a.bin

-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06100a.bin 2.11
pbif8x10_06100a.bin 2.24
pbifmrj_06100a.bin 4.04
pbifsp2_06100a.bin 4.02
statsmrj_06100a.bin 0.09
xgmacsp2_06100a.bin 0.17
xpp2x100_06100a.bin 1.05
xpp4x40_06100a.bin 6.10
xpp4x10g3_06100a.bin 5.00
xpp8x10_06100a.bin 1.08
xppmrj_06100a.bin 1.03
xppsp2_06100a.bin 1.01
xppxsp2_06100a.bin 1.01
pbif-ber-g3_06100a.bin 2.11
xpp20x10g3_npb_06100a.bin 7.13
xpp2x100g3_npb_06100a.bin 7.12

-DIRECTORY /FPGA/ManagementModule
mbridge32_06100a.xsvf 36
mbridge_06100a.xsvf 37
sbridge_06100a.mcs 6
hsbridge_06100a.mcs 17

-END_OF_IMAGES

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

```
xmlb06000.sig
xmb06000.sig
xmr06100a.sig
xmlp06100a.sig
lpfpga_npb_06100a.sig
hsbridge_06100a.sig
mbridge_06100a.sig
mbridge32_06100a.sig
sbridge_06100a.sig
pbif4x40_06100a.sig
pbif8x10_06100a.sig
pbifmrj_06100a.sig
pbifsp2_06100a.sig
pbif-ber-g3_06100a.sig
statsmrj_06100a.sig
xgmacsp2_06100a.sig
xpp2x100_06100a.sig
xpp20x10g3_npb_06100a.sig
xpp2x100g3_npb_06100a.sig
xpp4x40_06100a.sig
xpp4x10g3_06100a.sig
xpp8x10_06100a.sig
xppmrj_06100a.sig
xppsp2_06100a.sig
xppxsp2_06100a.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
xmr06100a.sha256
xmlp06100a.sha256
lpfpga_npb_06100a.sha256
hsbridge_06100a.sha256
mbridge_06100a.sha256
mbridge32_06100a.sha256
sbridge_06100a.sha256
pbif4x40_06100a.sha256
pbif8x10_06100a.sha256
pbifmrj_06100a.sha256
pbifsp2_06100a.sha256
pbif-ber-g3_06100a.sha256
statsmrj_06100a.sha256
xgmacsp2_06100a.sha256
xpp2x100_06100a.sha256
xpp20x10g3_npb_06100a.sha256
xpp2x100g3_npb_06100a.sha256
xpp4x40_06100a.sha256
xpp4x10g3_06100a.sha256
```

```
xpp8x10_06100a.sha256
xppmrj_06100a.sha256
xppsp2_06100a.sha256
xppxsp2_06100a.sha256

#  MIBS:
-DIRECTORY /MIBS
xmr06100a.mib
xmr06100a_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_06100a_mnf.txt
MLX_npb_06100a_mnf.sig
MLX_npb_06100a_mnf.sha256
```

FPGA file names for NPB and supported modules

File Name	Supported Modules
xpp20x10g3_npb_06100.bin	20x10G modules FPGA for NPB
xpp2x100g3_npb_06100.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 R06.1.00, 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 06.1.00.

NOTE: If you are not running one of the releases listed above, you CANNOT directly upgrade to 6.1.00.

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 06.1.00. Reload the device.

Scenario 3

To upgrade to 06.1.00 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 06.1.00 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

1. Upgrade to 06.1.00 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 NI 06.1.00.
3. Configure the **fpga-mode-npb** command and save the configuration.
4. Upgrade to the 06.1.00 NPB image using MLX_npb_06100_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@mlx16-1#show ver
System Mode: MLX
...
...
...
FPGA versions:
Valid PBIF Version = 2.11, Build Time = 8/19/2016 14:54:00

Valid XPP Version = 7.13 (NPB), Build Time = 10/13/2016 11:21:00
```

Output example for the show flash command

```
SSH@mlx16-1#show flash
...
...
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 8
Code Flash: Type MT28F256J3, Size 66846720 Bytes (~64 MB)
  o IronWare Image (Primary)
    Version 6.1.0T177, Size 9562733 bytes, Check Sum 9ee2
    Compiled on Dec  9 2016 at 04:55:10 labeled as xmlp06100b206
  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 6.0.0T175, Size 571513 bytes, Check Sum 4875
    Compiled on Jun  7 2016 at 16:09:50 labeled as xmlb06000
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 = 7.13 (NPB), Build Time = 10/13/2016 11:21:00
```

Output example for the show module command

```
SSH@mlx16-1#show module
Module                                                    Status
Ports    Starting MAC
M1 (upper):BR-MLX-MR2-M Management Module                 Active
M2 (lower):
F1: NI-X-HSF Switch Fabric Module                         Active
F2: NI-X-HSF Switch Fabric Module                         Active
F3: NI-X-HSF Switch Fabric Module                         Active
...
...
...
S4: BR-MLX-10Gx24-DM 24-port 10GbE Module                 CARD_STATE_UP
24       0024.387c.ee90
...
...
...
S8: BR-MLX-10Gx20 20-port 1/10GbE Module                  CARD_STATE_UP
20       0024.387c.ef50
```

OpenFlow upgrade and downgrade

When downgrading the system from R06.1.00 to R05.8.00, 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 only from 06.1.00 to 06.1.00a.

Limitations and restrictions

Compatibility and interoperability

- MLXe (NI006.1.00) and BFO 1.4 are interoperable.

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 06.1.00

TSB	Summary
TSB 2016-242-A [2]	A critical defect (DEFECT 617836) may cause unexpected MLX Line Card reloads due to some IPSec control packets received. This document is to provide urgent awareness of the software fixes available on MyBrocade for versions 5.8.00ec, 5.9.00be and 6.0.00ab. Brocade strongly recommends that all customers running the affected images upgrade to the fixed releases, **whether IPSec is configured or not.**
TSB 2016-240-A	To upgrade to R05.8.00 or any later release from releases prior to R05.6.00c, a two-step approach is required. The two-step approach involves upgrading first to R05.6.00c and then to the R05.8.00 or later release.

TSB issues outstanding in NI 06.1.00

TSB	Summary
None	

Closed with code changes R06.1.00a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 03/20/2017 in R06.1.00a.

Defect ID: DEFECT000621970	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** SSH - Secure Shell
Symptom: Management module may unexpectedly reload with below stack trace:- EXCEPTION 1200, Data TLB error Task : ssh_0 Possible Stack Trace (function call return address list) 20a7239c: ShFinishPacket(pc) 20a6b0bc: ShBuildDhKeyExchangeReply(lr) 20a6b0bc: ShBuildDhKeyExchangeReply 20a6e620: ProcessClientDhMessage 20a6d9ec: ShProcessMessage 20a76b20: ProcessClientInputData 20a76414: ShFiniteStateMachine 20979d98: HandleProtocolAction 20979b78: HandleConnectionTask 20a5c364: ssh_connection_task 20a5cab0: ssh_socket_control 20a5f718: ssh_receive_data_ready 20a5f75c: ssh_tcp_receive_data_ready_callback 20b55668: itc_process_msgs_internal 20b55b14: itc_process_msgs 20a57d24: ssh_in_task 00005e18: sys_end_task	
Condition: This can happen if a port scanning tool is scanning the SSH port on the device. The unexpected reset is seen after more than one SSH session has been opened and closed and while at least one session is active or in the process of being established. Note: - This defect is applicable for NetIron 05.8.00 and later releases up to and including 06.1.00.	
Workaround: Stop any known port-scanning tools scanning SSH port 22 to the device. Restrict SSH access only to authorized users by using access-list. To configure an ACL to permit allowed hosts, enter commands such as the following: device(config)# access-list 12 permit host x.x.x.x device(config)# ssh access-group 12 device(config)# write memory	

Defect ID: DEFECT000635645	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Ports behave unexpectedly. For example, IPv4 ACL configured on the port does not get applied to its traffic, VPLS local switched traffic egresses out of the port with a MPLS header, etc.	
Condition: Same IPv4 ACL is bound on more than one port on the same Packet Processor (PPCR).	
Workaround: Since binding one ACL on more than one port per packet processor (PPCR) triggers the issue, create one unique ACL for each port instead (even with the same rules) and apply them to individual ports.	

Closed with code changes R06.1.00

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 12/19/2016 in R06.1.00.

Defect ID: DEFECT000575987	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: OpenFlow scale numbers are not up to 64k.	
Condition: Specific to Management Module type MR2-X.	

Defect ID: DEFECT000577783	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: Port on 100Gx2-CFP2 line card module may not come up.	
Condition: Remote end CFP2 optic is removed and re-inserted.	
Recovery: Disable and enable the port on remote end.	

Defect ID: DEFECT000577992	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.8.00	**Technology:** OpenStack Integration
Symptom: The "flow-control/flow-control rx-pause ignore" status displayed in "show flow-cntrl" and "show interface" is not in sync with the "flow-control/flow-control rx-pause ignore" configuration.	
Condition: On executing below commands to see flow-control status: 1. show interface 2. show flow-cntrl	

Defect ID: DEFECT000578252	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** VLAN - Virtual LAN
Symptom: Flapping of VLL	
Condition: When VRF is moved from one interface to another interface belonging to different PPCR.	
Workaround: While moving VRF from one interface to another belonging to different ppcr, disable both interfaces and then move the VRF.	

Defect ID: DEFECT000578821	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Hardware Monitoring
Symptom: 100G CFP2 port goes down and LED may still glow green	
Condition: 100G CFP2 port status is down on both sides	

Defect ID: DEFECT000579744	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** CLI - Command Line Interface
Symptom: Management Module may reload unexpectedly while executing concurrent show commands from multiple sessions like TELNET, SSH.	
Condition: Multiple show commands should be executed from different sessions while a "write memory" command is executed. Example: "show lag", "show ip ospf interface", "show ipv6 bgp summary"	

Defect ID: DEFECT000581204	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** OAM - Operations, Admin & Maintenance
Symptom: Link of 100Gx2-CFP2 LR4 interface may go down.	
Condition: 1. When the RX side of the cable connected to the remote end was removed. 2. When the remote end device is from a particular third-party: WDM/DTN-X.	
Recovery: Remove and Re-insert of the TX cable from the remote end.	

Defect ID: DEFECT000583134	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.1.00	**Technology:** ACLs - Access Control Lists
Symptom: When IPv6 ACL is applied on a VEoVPLS interface, deny Logging syslogs aren't generated.	
Condition: IPv6 ACL deny logging doesn't generate any syslogs when applied on a VEoVPLS interface.	

Defect ID: DEFECT000584408	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: During system bootup, when MP configuration is being synchronized to all LPs, one or more of the LPs go for an unexpected reload with scaled number of ACLs and PBR bound to multiple interfaces	
Condition: This problem can be seen In a system with scaled number of ACLs configured and PBR bound to multiple interfaces on multiple LPs.	

Defect ID: DEFECT000586053	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: ACL Rules fail to sync from management module to some of the line cards within a scaled configuration of MAC/IPv4/IPv6 ACLs.	
Condition: With a scaled number of MAC/IPv4/IPv6 ACLs, management module takes significant amount of time to complete synchronization of the configuration to all the Linecards. In rare conditions, the synchronization of configurations can fail, resulting in the ACL configuration not being present in the Linecard.	

Defect ID: DEFECT000587069	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.4.00	**Technology:** VLAN - Virtual LAN
Symptom: When configuring a new VLAN on the CES, the "Error: insufficient fids available for vlan creation" message appears	
Condition: On CER/CES platform, with continuous churns due to multicast traffic sources and receivers	

Defect ID: DEFECT000587126	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** VPN
Reported In Release: NI 05.6.00	**Technology:** EVPN - Ethernet VPN
Symptom: When "default-local-preference" parameter is globally set, the VPNV4 advertised aggregate routes will not update the local-pref with the new parameter set, even after clearing the BGP neighborship using "clear ip bgp neighbor all"	
Condition: Aggregate routes are advertised through BGP VPN. "default-local-preference" should be globally set/reset	
Workaround: Run "clear ip bgp vrf <vrf-name> neighbor all" for the VRF's associated. (or) Remove & add "local-as" under "router bgp" which stops and then restarts the BGP operation.	

Defect ID: DEFECT000587263	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** PBR - Policy-Based Routing
Symptom: Device takes a long time to stabilize and recover the traffic after system reload with scaled ACL configuration	
Condition: This issue is seen only in scaled scenario. If user has scaled route-map configuration the reload time will increase proportionally.	
Recovery: System will recover by itself.	

Defect ID: DEFECT000589935	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Sometime IPsec Module may reset when the following commands are issued using script: no interface tunnel <tunnel-number> no ipsec profile <ipsec-profile-name> no ikev2 profile <ikev2-profile-name> no ikev2 policy <ikev2-policy-name> no ikev2 auth-proposal <auth-proposal-name> no ikev2 proposal <ikev2-proposal-name>	
Condition: Issue the following commands using script with no delay between each command: no interface tunnel <tunnel-number> no ipsec profile <ipsec-profile-name> no ikev2 profile <ikev2-profile-name> no ikev2 policy <ikev2-policy-name> no ikev2 auth-proposal <auth-proposal-name> no ikev2 proposal <ikev2-proposal-name>	

Defect ID: DEFECT000590355	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS Traffic Engineering
Symptom: This occurs with a scaled scenario on a slow server with a response time longer than 10 seconds. No path is available for the LSPs, so the LSPs keep retrying.	
Condition: The server response time should be within milliseconds. This is one of the main reasons to use PCE. The issue was seen only when using a third party test emulator.	

Defect ID: DEFECT000590434	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** sFlow
Symptom: Management Module may reload unexpectedly when an sFlow sample is being processed.	
Condition: "sflow forwarding" should be enabled on the interface and "vrf forwarding <vrf-name>" should be enabled on the corresponding VE in which the interface is a member.	

Defect ID: DEFECT000591098	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** IPv4 Multicast Routing
Symptom: Video freezes every 3 minutes	
Condition: In ring topology where the RPT and SPT path is different and when ASSERT winner becomes blocked OIF on (S,G) entry	

Defect ID: DEFECT000591161	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: Sometimes BFD session flaps when Openflow-flows are deleted using "clear open all" command.	
Condition: When Openflow-flows are deleted using the command "clear open all".	
Recovery: BFD session will recover by itself.	

Defect ID: DEFECT000591202	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** CLI - Command Line Interface
Symptom: Multiple interfaces stay down on MLX 10Gx20 with 1G SFPs and do not come up even on disable/enable.	
Condition: The issue is seen when - chassis is loaded with default config, - MLX 10x20G card is inserted without the optics, and - 1G SFPs are then inserted fairly fast on the interfaces	

Defect ID: DEFECT000591211	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: The below i2c access syslog/trap messages for PSUs will be observed. SYSLOG: <174>Jan 30 03:22:39 mlxe3 System: i2c access notice (GIEI = set)Minor, Mux index 0, Mux tap 5, ID 0x1, Addr 0x5, (PS2) SYSLOG: <174>Jan 30 03:22:39 mlxe3 System: i2c access notice (GIEI = clear)Minor, Mux index 0, Mux tap 5, ID 0x1, Addr 0x5, (PS2)	
Condition: On running "show chassis" command continuously with all PSUs present in the chassis.	

Defect ID: DEFECT000591955	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: Incorrect metric value might be advertised for a BGP route to a EBGP neighbor, with the neighbor configured without route-map.	
Condition: The neighbor should have an out route-map, The route-map should have "set metric-type internal" which will advertise the BGP route with IGP metric for MED.	
Workaround: "clear ip bgp neighbor <neighbor address > soft out"	

Defect ID: DEFECT000592732	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS Traffic Engineering
Symptom: When a second IP address is configured for an interface, it is possible RSVP chooses the second IP address while sending back a RESV. When upstream router processes the RESV message, it drops the message because it does not match the RRO it was expecting. Thus the LSP will not come up.	
Condition: This is a rare occurrence.	
Workaround: Unconfiguring the second interface IP address will bring up the LSP.	

Defect ID: DEFECT000592929	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Unexpected reload of line card module.	
Condition: Loopback interface in non-default VRF has the same IP address as that of the loopback interface in default VRF.	
Workaround: The IP addresses of loopback interfaces in default and non-default VRF need to be different.	

Defect ID: DEFECT000593035	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** LAG - Link Aggregation Group
Symptom: In a VPLS network, multicast destined packets may go on wrong VPLS instance on the remote PE.	
Condition: In a VPLS network with "vpls-cpu-protection", multicast destined packets may go on wrong VPLS instance on the remote PE when a user disables and re-enables one of the forwarding paths.	
Recovery: Problem can be recovered by reloading the device.	

Defect ID: DEFECT000594037	
Technical Severity: Medium	**Probability:** High
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: There are sometimes a lot of SYSLOG messages indicating OSPFv3 LSA re-transmission.	
Condition: This happens if "log-status-change" is enabled in OSPv3 config to enable LSA-retransmit traps.	

Defect ID: DEFECT000594398	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Hardware Monitoring
Symptom: Parity error similar to below mentioned is seen in syslog: Mar 24 09:15:42:E:CAM2PRAM Word 2 Double Bit Parity Error on port range 1/1 - 1/10	
Condition: Single bit ECC error occurs on the Linecard module NP memory.	

Defect ID: DEFECT000594606	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: A Line card software exception occurred with the below syslog and stack trace without any user intervention. SYSLOG: <141>Mar 27 08:56:30 R50-MLXe8 System: Module down in slot 5, reason CARD_DOWN_REASON_REBOOTED. Error Code 0 Stack Trace: ========== Possible Stack Trace (function call return address list) 00000000: .zero(pc) 20c18bec: ipc_multi_module_handler(lr) 20c1b1f0: ipc_process_messages 20c1b9cc: ipc_receive_packet 20036d14: ge_process_ipc_data_msg 207f57b4: lp_ipc_task 00040158: sys_end_task	
Condition: LP SW exception will occur while handling message from Management Module. This condition was created when BGP neighbor was flapping on management module and was sending lots of rout e update to LC	
Recovery: The Line card will reboot and come up	

Defect ID: DEFECT000595113	
Technical Severity: High	**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: When the router is acting as DHCPv6 relay agent, it is not choosing DHCPv6 client facing interface's link-local address as the source address in the IPv6 packet when it forwards reply message to the client.	
Condition: The device should act as a DHCPv6 relay agent.	

Defect ID: DEFECT000595261	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Multicast source lookup fails due to unavailability of unicast routes in the system.	
Condition: This issue introduced when unicast traffic does not have the routes in routing table that are required for multicast source and RP lookup.	
Workaround: Make sure unicast routing table is populated before running multicast traffic.	

Defect ID: DEFECT000595638	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: DUT might experience a unplanned restart when more than 32K OpenFlow flows are being configured over SSL.	
Condition: More than 32K flows are sent from OpenFlow controller.	

Defect ID: DEFECT000595704	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: Unable to establish TCP connection over GRE Tunnel.	
Condition: The command "ip tcp redirect-gre-tcp-syn" should be present in the global configuration, while the tunnel source port should have the command "ip tcp adjust-mss <value>" enabled.	
Workaround: Remove the command "ip tcp adjust-mss <value>" from the interface configuration.	

Defect ID: DEFECT000595910	
Technical Severity: Medium	**Probability:** High
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: Extraneous config lines are added to running-config starting with "no trap ----".	
Condition: This happens after a reload if OSPFv3 "log-status-change" is configured.	

Defect ID: DEFECT000595942	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS Traffic Engineering
Symptom: System reset is seen sometimes when select-path is retrying a new instance due to an IGP neighbor down event and no path is available.	
Condition: The system has IGP sync enabled and an LSP has selected a path as the Active path. In addition there is no alternative path for the selected secondary to come UP. Under these conditions, if an interface flap in the network triggers a neighbor down event, this issue may be seen.	

Defect ID: DEFECT000595982	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: BFD session state is staying UP even after un-tagging the port from VLAN.	
Condition: Sometimes after untagging a port from VLAN.	
Recovery: Execute the below command after untagging ports from VLAN if a BFD session state does not transition to DOWN state "clear bfd neighbors A.B.C.D/X:X::X:X"	

Defect ID: DEFECT000596106	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: When MPLS is running with OSPF as IGP, changing OSPF network type causes Dynamic Bypass LSPs to get created. These get deleted after a few seconds since they don't get used by Backup paths. This process of creation/deletion repeats.	
Condition: 1) MPLS is running with OSPF as IGP 2) Dynamic bypass is configured 3) OSPF network type is changed from broadcast to p2p without bringing down the interface state	

Defect ID: DEFECT000596110	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** LAG - Link Aggregation Group
Symptom: A LAG can be deployed with inconsistent sFlow configuration on primary port and secondary port.	
Condition: "sflow forwarding" is enabled on an interface and is added to a deployed LAG whose primary port does not have it enabled. Note: This does not affect the LAG configuration	

Defect ID: DEFECT000596196	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** Syslog
Symptom: Alarm messages similar to the ones given below will be seen in Syslog/LP console along with trap message when 10GE Tunable SFP+ optics are connected. Apr 20 14:17:38:A: Latched low RX Power alarm, port 1/3 Apr 20 14:17:38:A: Latched low RX Power alarm, port 1/1	
Condition: Tunable Optic SFPs connected	
Recovery: "dm optic <port> eeprom" command can be executed on the associated Linecard Module to suppress the alarm messages in the Syslog.	

Defect ID: DEFECT000596208	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: The router inexplicably restarted.	
Condition: When BFD sessions are established over LAG ports.	

Defect ID: DEFECT000596213	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: In rare corner cases, the following error messages appear and the "enable" prompt can't be reached. Error:send_port_state_down_event: Sync to standby MP failed (err = Timeout) Warn:send_port_state_up_event: Sync to standby MP failed (err = Timeout) Error:send_port_state_down_event: Sync to standby MP failed (err = Timeout) Warn:send_port_state_up_event: Sync to standby MP failed (err = Timeout) Error:send_port_state_down_event: Sync to standby MP failed (err = Timeout)	
Condition: System is a scaled setup having 4k vlan, ipv6, ipv4, vpls, mpls, muticast, ipsec features running. The issue is seen after reload of the setup.	
Workaround: No Workaround	
Recovery: Reload the router	

Defect ID: DEFECT000596312	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: Link SFM 1/FE 1/Link 1 will be put to DOWN state with following message due to side effect of auto tuning. Warning: Fabric Link shutdown due to Autotuning failure for SFM 1/FE 1/Link 1 -> LP 1/FE 1/Link 76	
Condition: Link SFM 1/FE 1/Link 1 will be put to DOWN state when auto-tuning fails.	
Recovery: Power on link SFM 1/FE 1/Link 1 manually.	

Defect ID: DEFECT000596446	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS Traffic Engineering
Symptom: After a request has been made, if the user disables the LSP, removes 'pce compute' from the LSP config and enables it, and the response comes or timeout occurs, the error code of the LSP will be incorrect. This happens in scenarios where the server response is very slow, in the order of 10s of seconds, or when the request is timed out due to unresponsive server.	
Condition: Seen only with PCE servers with extremely slow response time, or when the request is timed out as per the request timer, and the user changes the config on the LSP during this time to make the LSP locally computed.	

Defect ID: DEFECT000596574	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.9.00	**Technology:** Traffic Queueing and Scheduling
Symptom: TM errors on a 32-slot chassis with 24x10G modules resulting in traffic drop.	
Condition: Seen on a 32-slot chassis with 24x10G modules present. Triggered by either - a chassis reload or - an LP insertion while traffic is present, or - an LP reboot while traffic is present.	
Workaround: For the chassis reload - Add the command "wait-for-all-cards" in the configuration before reload. This will ensure that the issue does not happen during chassis reload. For LP insertion - If LP is inserted without any config present for the LP, the issue will not happen. If LP is inserted with a config present for the LP, the issue can happen and recovery will need to be performed.	
Recovery: Reload the chassis after configuring the "wait-for-all-cards" command.	

Defect ID: DEFECT000597413	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** Configuration Fundamentals
Symptom: Link fault signaling settings are not applied after reloading the chassis.	
Condition: With link fault signaling enabled globally either of the following conditions can cause this issue: - - A new Linecard Module is inserted - Existing Linecard Module is power cycled - Chassis is reloaded	
Recovery: Disable and enable link-fault-signaling globally	

Defect ID: DEFECT000597682	
Technical Severity: Critical	**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: OSPFv3 task could cause router to unexpectedly reload	
Condition: If the OSPFv3 task receives multiple external LSAs with Forwarding Address field and if the longest prefix match for the Forwarding Address in OSPFv3 is in an area not same as ASBR (external LSA originator)	

Defect ID: DEFECT000597791	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** IP over MPLS
Symptom: MPLS Traffic forwarding failing on MPLS transit node after reloading or inserting ingress Linecard module.	
Condition: Reload or insertion of Linecard module which has MPLS configuration.	
Recovery: Disable and enable the outgoing interface so that it would clear the existing ARP entries and relearn it.	

Defect ID: DEFECT000597936	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.4.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Customer not able to fetch the VRRP related information (vrrpAssoIpAddrTable, vrrpRouterStatsTable) through SNMP.	
Condition: When VRRP is configured and during polling the VRRP related information (vrrpAssoIpAddrTable, vrrpRouterStatsTable) through SNMP.	

Defect ID: DEFECT000598531	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Incorrect ACL index displayed in the running configuration	
Condition: When 4K ACLs are supported and sequence numbers greater than 2^18 are used for the filters	

Defect ID: DEFECT000599092	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: New half-height line card module comes up on a slot blocked for a full height card 2x100G	
Condition: 2x100G line card is configured manually. New half-height line card module when inserted on the slot which is blocked for full height card 2x100G	

Defect ID: DEFECT000599156	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.7.00	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: The CLI prompt is displayed when providing the wrong credential during the telnet authentication.	
Condition: During the telnet authentication, continuous "?\n" is entered on the login prompt.	

Defect ID: DEFECT000599286	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: TACACS+ server accounting log displays the password in plain text.	
Condition: TACACS+ accounting is configured and any command that has password associated with it is executed from CLI.	

Defect ID: DEFECT000599540	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.7.00	**Technology:** ACLs - Access Control Lists
Symptom: Erroneous counting of IPv6 traffic results in incorrect rate limiting of the received traffic and hence packet drops	
Condition: IPv6 ACLs with rate limiters should be configured along with IPv4/Port level rate limiters Modification (Delete/Add) of IPv4/Port level rate limiters	
Recovery: Reload of the affected Linecard Module is the only option	

Defect ID: DEFECT000599891	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 06.0.00	**Technology:** Rate Limiting and Shaping
Symptom: Unable to un-configure "rate-limit ce-refresh-intrv" by disabling "qos-pol"	
Condition: disabling "qos-pol" before disabling " rate-limit ce-refresh-intrv"	
Workaround: disable "rate-limit ce-refresh-intrv" before disabling "qos-pol"	

Defect ID: DEFECT000600100	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** PBR - Policy-Based Routing
Symptom: The output of the show command "show packet-encap-processing" also displays slot information of the slots which do not have packet-encap-processing features configured on them.	
Condition: Configure packet-encap-features on 1 slot out of 2 or more slots present in the MLX device. Then execute the command "show packet-encap-processing".	

Defect ID: DEFECT000600108	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: Not able to enable the configuration for generating the PCEP traps through CLI command "snmp-server enable traps pcep".	
Condition: When trying to enable the configuration for generating PCEP traps, through the CLI command "snmp-server enable traps pcep".	
Workaround: Need to use the CLI command "snmp-server enable traps mpls pcep" to enable the configuration for generating the PCEP traps.	

Defect ID: DEFECT000600151	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** IPsec - IP Security
Symptom: Unexpected reload of standby Management module.	
Condition: This issue may be observed when a large number of IPsec tunnels are configured and the IPSEC re-keying mechanism is in progress.	

Defect ID: DEFECT000600153	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: Enabling OpenFlow on the LAG's primary port may transition LAG ports into LACP blocked state.	
Condition: OpenFlow configuration on primary port of a LAG is prerequisite. Enable OpenFlow on the primary port of a LAG. Witness the LAG ports going into LACP blocked state.	

Defect ID: DEFECT000600155	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: LAG undeploy is blocked after OpenFlow is disabled on primary port of the LAG	
Condition: Enable OpenFlow on a LAG primary port. Disable OpenFlow from the LAG primary port. Try to undeploy the LAG, witness LAG undeploy is blocked by openflow.	

Defect ID: DEFECT000600170	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: Trigger OpenFlow "mpls-us-enable" enable/disable command on CLI continuously, BFD may flap at a point of time.	
Condition: Configure OpenFlow mpls-us-enable with BFD enable in system.	
Workaround: Use High BFD timeout value say 2 sec.	

Defect ID: DEFECT000600232	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Packet in L2VPN payload is reformed as L3 and hence causing some packets to drop at the egress device	
Condition: This issue will happen when an OpenFlow rule is created with L2VPN label in action.	

Defect ID: DEFECT000600325	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: After an MP Switchover - observe MCT VPLS traffic drop	
Condition: MP switchover with MCT VPLS config	
Workaround: use "clear mac address vpls" command.	

Defect ID: DEFECT000600352	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: The configuration "lag primary-port-dynamic" enables the user to change the primary port on a deployed LAG. This support not being enabled on SNMP, the user would see the following error when tried to change the primary port of a deployed LAG. Error in packet. Reason: not Writable	
Condition: The error can be encountered when attempted to change the primary port of a deployed LAG with primary-port-dynamic enabled.	

Defect ID: DEFECT000600532	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** MAC Port-based Authentication
Symptom: When “delete-dynamic-learn" is enabled under "global-port-security", MAC addresses learned on a PMS enabled LAG do not get deleted when the LAG goes down.	
Condition: Under "global-port-security", "delete-dynamic-learn" is enabled. PMS is enabled on a LAG port. MAC addresses are learned on LAG's member ports. LAG is either disabled or goes down	
Recovery: Delete the Secure MAC address learned on the LAG manually.	

Defect ID: DEFECT000600814	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** OAM - Operations, Admin & Maintenance
Symptom: In the output of "show media", the dual rate 10G/1G optic transceiver module type is shown as unknown	
Condition: The speed has to be configured as 1000-full and linecard module has to be reloaded. This issue is specific to 20x10G linecard module.	
Recovery: Remove the speed configuration - 1000-full.	

Defect ID: DEFECT000600930	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: In some cases, the DHCP clients will not get the address from the server when the MLX is acting as a relay agent.	
Condition: The VE interface is configured with an IP unnumbered loopback. MLX receives a DHCP discovery packet with option-82 and option-43 already inserted.	
Workaround: Move the IP address from the loopback interface to the VE interface. Disable option 82.	

Defect ID: DEFECT000601056	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: A deployed LAG must always have a primary port. The feature "port-primary-dynamic" enables election of the primary port, among the ports configured for the LAG. Since the feature was not supported in SNMP, it would accept and configure the primary port to zero.	
Condition: With the configuration "lag port-primary-dynamic" enabled, SNMP may accidentally set primary port to 0.	

Defect ID: DEFECT000601068	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: CLI rejects no-deploy when 2 or more ports of the LAG are enabled. SNMP had no such restriction unlike CLI	
Condition: Setting LAG status to No-deploy from SNMP, for a LAG which has 2 or more of its ports enabled, would be accepted without any errors	

Defect ID: DEFECT000601178	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: Convergence timer is higher for a FRR enabled LSP.	
Condition: This happens when a MM switch-over is performed on an intermediate node in a LSP path.	

Defect ID: DEFECT000601298	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** sFlow
Symptom: sFlow samples sent to sFlow collector are corrupted	
Condition: Interface is configured with sFlow sampling and IPv6 ACL.	

Defect ID: DEFECT000601379	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP OID mplsLspAutoBWSampleRecordingEnable output for "sample-recording" field does not match the corresponding CLI output for "show mpls lsp name <lsp_name> auto" command	
Condition: MPLS LSP primary path is configured and sample recording is disabled on the primary path using CLI.	

Defect ID: DEFECT000601542	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** IPsec - IP Security
Symptom: Unexpected reload of standby Management module.	
Condition: This issue may be observed when a large number of IPSEC tunnels are configured and IPSEC re-keying mechanism is in progress.	

Defect ID: DEFECT000601596	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Software Installation & Upgrade
Symptom: When issuing the format command for CF slot1 or slot2, via SSH, the system might not format the CF module at all.	
Condition: Conditions were unclear, the probable scenario is this, "if the PCMCIA card is being used for any copy operation from a different session (telnet/SCP), the device is in use. Hence the 'format' command does not work."	
Workaround: Do not format the card when it is in use (might be from a different session).	
Recovery: Close all the open sessions, this would terminate the unknown copy operations happening on the card, or reload the chassis and then format the PCMCIA card.	

Defect ID: DEFECT000601634	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: On CES/CER, IP multicast traffic received on ICL port will be forwarded to local CCEP even though remote CCEP is UP.	
Condition: Add a member-VLAN to the MCT cluster.	
Recovery: Save the new configuration & Reload.	

Defect ID: DEFECT000601641	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.4.00	**Technology:** High Availability
Symptom: Intermittent issues in management connectivity	
Condition: If there are ARP requests being sent to target IP address 0.0.0.0, the Standby management module may respond to them	

Defect ID: DEFECT000601776	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP OID 1991.1.1.2.1.44.0 displays value as "Reason: Unspecified" instead of "Reason : Fabric connectivity up"	
Condition: When fabric connectivity transitions from down to up	

Defect ID: DEFECT000601789	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv4 Multicast Routing
Symptom: Unexpected reload of standby Management module.	
Condition: This issue may be observed when a large number of IPSEC tunnels are configured and IPSEC re-keying mechanism is in progress.	

Defect ID: DEFECT000601805	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Syslogs are not generated for IPv4 RACL permit logging.	
Condition: Bind IPv4 RACL before creating the IPv4 ACL	
Workaround: Execute "ip rebind-receive-acl all" or Unbind and then bind receive ACL after the acl is created.	

Defect ID: DEFECT000601808	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Sample-recording functionality does not work when auto-bandwidth enabled secondary path of an LSP is activated even with sample-recording configured.	
Condition: Secondary path on which auto-bandwidth is enabled with sample-recording feature gets activated.	
Workaround: Create a template with sample recording enabled and apply to the secondary path	
Recovery: Create a template with sample recording enabled and apply to the secondary path	

Defect ID: DEFECT000601841	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Standby MP software exception is observed and MP will reload	
Condition: 'Deploy' and 'No Deploy force' SNMP requests for a LAG, with very less time gap between the commands, on a loaded setup will cause software exception on the standby MP.	

Defect ID: DEFECT000601969	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Permit logging doesn't work on traffic received on secondary ports of the LAG.	
Condition: Permit logging is configured on primary port of a LAG and traffic is received on the secondary ports.	

Defect ID: DEFECT000602060	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 06.0.00	**Technology:** MRP - Metro Ring Protocol
Symptom: Interface statistics shows packet counts more than expected after switchover.	
Condition: This may be seen some times when switchover is done with MRP configurations.	

Defect ID: DEFECT000602382	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** LAG - Link Aggregation Group
Symptom: Unable to "deploy" or "no deploy" a LAG. The following timeout message is seen - Error: Timed Out LAG ABCD deployment failed!	
Condition: When the following are all true - - System has undergone port flaps, LAG member updates, and other timer events such that the timer identifier value has gone past value 4294967295. - "delay-link-timer" is configured	

Defect ID: DEFECT000602394	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** ICMP - Internet Control Message Protocol
Symptom: Brocade's NetIron OS is susceptible to CVE-2016-1409 (IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability). A vulnerability in the IP Version 6 (IPv6) packet processing functions could allow an unauthenticated, remote attacker to cause an affected device to experience elevated CPU usage on the management module.	
Condition: Reception of IPv6 ND6 packets with Hop Limit set as 255.	
Workaround: On GEN3 module, apply User Defined ACL (UDA) to filter out invalid ND6 packets in the hardware with software release 5.9 or later.	

Defect ID: DEFECT000602475	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: When "mpls-unknown-label-forward" configuration is applied, the packets are getting dropped in the transit node.	
Condition: Enabling "openflow mpls-us-enable" configuration made the non-openflow ports to behave as openflow MPLS.	

Defect ID: DEFECT000602514	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VLL - Virtual Leased Line
Symptom: CER device may reload upon deletion of MCT VLL peer configuration	
Condition: Deletion of MCT-VLL peer configuration	

Defect ID: DEFECT000602818	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Telemetry
Symptom: ACLs do not work and no traffic is forwarded. No CAM entries found in line cards.	
Condition: A memory leak in the line-card can cause memory allocation to fail and the line card becomes unable to store the ACL entries received from management module. Since the ACL rules are not downloaded, they are not programmed in the hardware. The memory leak is caused by updates in the next hop VLAN of the route map where the ACL entries are present. This can be triggered by events such as port flap on the line card in question, reloads of other line cards in the system and updates in the VLAN configuration.	

Defect ID: DEFECT000602832	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: When OpenFlow rules are configured in reverse order of priority, there can be 100% traffic loss.	
Condition: 1. Configure OpenFlow rule with priority 100 2. Configure OpenFlow rule with priority 90 3. Observe 100% traffic loss on the first OpenFlow rule.	
Workaround: Apply OpenFlow rules in ascending priority order, i.e., first apply rule with priority 90 and then priority 100.	

Defect ID: DEFECT000602865	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: When OpenFlow rules are configured in reverse order of priority, complete traffic loss may be observed.	
Condition: 1. Configure OpenFlow rule with priority 100 2. Configure OpenFlow rule with priority 90 on the same port. 3. Observe complete traffic loss.	
Workaround: Apply OpenFlow rules in ascending priority order, i.e., first apply rule with priority 90 and then priority 100.	

Defect ID: DEFECT000602912	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 06.0.00	**Technology:** LAG - Link Aggregation Group
Symptom: rate-limit configuration not reflecting properly on a LAG. "show rate-limit" command output also does not display the rate-limit configuration.	
Condition: When port-primary-dynamic feature is enabled and when primary port is changed dynamically after deployment. Note: this defect is applicable from 6.0 release onwards	
Recovery: Configure the rate-limit parameters on the LAG again (after changing the primary port)	

Defect ID: DEFECT000602943	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IGMP - Internet Group Management Protocol
Symptom: Invalid IGMP static group IP address (syntactically invalid) is accepted in CLI and shown in running configuration. For example, if user enters mcast grp ip 244.10.10.1 as 244.10.101 the CLI will be accepted.	
Condition: While configuring IGMP static entry, device will accept a syntactically incorrect group IP address.	

Defect ID: DEFECT000602988	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: VLL Traffic loss will occur when VLL instances are removed and then added back	
Condition: Removing VLL instances and then re-added via SCP.	
Recovery: Reload the device where VLL instances were removed and added back.	

Defect ID: DEFECT000603088	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Deny logging syslog messages aren't generated when enabled for IPv6 receive ACLs	
Condition: This can occur when user configures IPv6 receive ACL and enables IPv6 receive ACL deny logging.	

Defect ID: DEFECT000603095	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: Device unexpectedly reloads	
Condition: (1) Have 2 ASBRs in 2 different areas (ex: area-0 & area-200) and there is a ABR connecting the ASBRs in those respective areas. (2) Have both the ASBRs originating the same external destination (x.x.x.0/24) one with forwarding address set and the other not set. (3) when configuration rfc1583 is disabled on the ABR	
Workaround: enable rfc1583 on the ABR	

Defect ID: DEFECT000603131	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** FDP - Foundry Discovery Protocol
Symptom: Even after FDP is disabled locally on the primary port of a LAG, the secondary ports of the LAG are listed as FDP neighbors on other devices.	
Condition: After disabling FDP on the Primary port of a LAG the Active Management Module must be reloaded	
Recovery: Enable and disable FDP on the primary port of the LAG	

Defect ID: DEFECT000603263	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: When an OpenFlow rule with action send to controller is present and if the LC is reloaded, the traffic will not hit the OpenFlow rule even after LC is up.	
Condition: 1.Create OpenFlow rule with action send to controller. 2. Reload LP. 3. After LP is up, witness traffic drop.	

Defect ID: DEFECT000603611	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: A /32 stale T3-LSA will remain in the area-0 DB even though all the contributing routes are removed from the other area.	
Condition: (1) Configure the 3 IP addresses in some order on interfaces of 3 different routers in some area (e.g., 2000) with the subnets labeled in a manner similar to this: x.y.z.221/32, x.y.z.221/31, x.y.z.222/30. (2) Delete the above configured interfaces in some order to hit this issue.	

Defect ID: DEFECT000603644	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.8.00	**Technology:** QoS - Quality of Service
Symptom: QoS statistics on egress ports always shows against Queue 0	
Condition: CLI Command "extended-qos-mode" should be configured on the device.	

Defect ID: DEFECT000603754	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: Customer may not see syslog when SSL session gets closed due to some issues. When a controller or its TCP/IP stack runs into an issue and terminate the TCP or SSL session, this remote event was not handled by the switch to log the informational event of closing the connection. While normal close and keep-alive timeout have been handled and working.	
Condition: Abnormal closure of SSL/TCP connection initiated by the OpenFlow controller. This event might not be logged by the switch.	

Defect ID: DEFECT000603801	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** High Availability
Symptom: Standby MP resets silently while running the script containing the clearing of multiple protocols' data (bgp, ospf , mpls LSP and VPLS Mac) in quick succession	
Condition: Repeatedly clean multiple protocols' data (bgp, ospf , mpls LSP and VPLS Mac) by running a script with few seconds gap between each CLI command.	
Workaround: Increase the timegap between the CLI commands.	

Defect ID: DEFECT000603818	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: MCT Cluster will not be deployed after MP switchover.	
Condition: "No deploy" LAG which is used as ICL in MCT Cluster.	

Defect ID: DEFECT000603899	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: Unexpected reload of management module on MLX when loading the start-up configuration file. Possible Stack Trace (function call return address list) 201171e0: copy_startConfig_runConfig(pc) 201171dc: copy_startConfig_runConfig(lr) 20117968: init_runConfig_from_startConfig 20177358: console_task 00005e18: sys_end_task	
Condition: When loading start-up configuration file with 100K ACLs.	

Defect ID: DEFECT000603982	
Technical Severity: Low	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: When a passive OpenFlow connection is configured, ip-address can be optionally specified. This ip-address is intended to specify which local (in switch) ip-address to listen to. The issue is that even if ip-address is specified, it still accepts connection on any local ip-address. So, any controller can still connect to the switch on non-specified IP address, as the passive connection listens to any ip-address.	
Condition: When local ip-address is specified in passive OpenFlow connection, it is supposed to only listen to that ip-address. Instead, it simply ignores the local IP address configuration and accepts OpenFlow connections on any local IP address.	

Defect ID: DEFECT000604050	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** Static Routing (IPv6)
Symptom: On a CER/S device, when an IPv6 static route entry exists and a new IPv6 static route is added (less or more specific for the existing prefix), traffic pertaining to that prefix is either dropped OR forwarded on the interface associated with the old entry	
Condition: When an IPv6 static route entry exists and a new IPv6 static route is added (less or more specific for the existing prefix) Note: Issue is applicable only for CER/S devices	
Workaround: Remove the existing IPv6 static route and then add the new entry	
Recovery: Remove both the IPv6 static routes (old and new) and apply the new entry again	

Defect ID: DEFECT000604087	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** OSPFv3 - IPv6 Open Shortest Path First
Symptom: The OSPFv3 ABR did not install a more specific route learned from another area when the more specific route that it learns falls within the same area range configured on this router.	
Condition: (1) area range on an OSPFv3 ABR is configured and it originates T3-LSA into backbone for area-range summary and installs this route into RTM. (2) Another ABR originates a more specific route that falls within the configured area-range on the first ABR.	

Defect ID: DEFECT000604159	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: OpenFlow matched traffic is forwarded to any one of the 8 queue, when flows are added with invalid queue-id (> 8).	
Condition: Flow addition/modification with Invalid queue-id in its action	
Recovery: This issue has been fixed in current release	

Defect ID: DEFECT000604313	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** PBR - Policy-Based Routing
Symptom: L2PBR binding not propagated to Linecard. Memory leak on line card when L2PBR is bound on the interface. IPv4 PBR entries are not programmed to TCAM.	
Condition: L2PBR binding isn't propagated to Linecard when binding is performed before defining the route-map. Memory leak on the Linecard when L2PBR is applied on the interface. IPv4 PBR entries aren't programmed to hardware when the same route-map is bound on the same interface for L2PBR.	
Workaround: Define route-map before binding on interface for L2PBR entries to be programmed.	

Defect ID: DEFECT000604330	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.7.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP OID "snSwIfInfoGigType" returns the value as unknown(255)	
Condition: When polling OID "snSwIfInfoGigType", for Finisar 10G SR SFP+ optic configured with "speed-duplex 1000-full" it returns the value as unknown(255)	

Defect ID: DEFECT000604628	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: A system reload happens when debug destination is SSH, enable "debug ip pim oif add-del" and clearing PIM mcache.	
Condition: If PIM is enabled and debug output is sent to SSH.	

Defect ID: DEFECT000604894	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.7.00	**Technology:** MPLS Traffic Engineering
Symptom: Below symptoms are seen on router with MPLS Traffic Engineering configured with OSPF-TE as IGP. 1. Memory Allocation Failures console prints will be seen on Router. 2. Router Active Management Module goes to low available memory, less than 20%. Brocade#show memory ... Available Memory (%): 20 percent ... 3. Large number (greater than 15,000) of allocations seen for TE-LSA-Id elements in MPLS; Alloc field of TE-LSA-Id in below command output Brocade#show mpls memory ... Mem-Type Alloc BytesAlloc TotalAlloc TotalFree AllocPeak AllocFail FreeFail ... TE-LSA-Id 10145010 578265570 10426232 281222 10145010 0 0 ... Large number of TE-LSA-Id allocations implies that many of its allocations were not freed when they were supposed to be freed. Memory Allocation failure in MPLS will lead to unspecified behaviors like CSPF fail, LSP not coming up, Fast reroute not happening,	
Condition: Above mentioned Symptoms will be seen on router only with below conditions 1. MPLS Traffic Engineering configured using OSPF TE. Brocade(config-mpls-policy)#traffic-engineering ospf area [area-id] 2. A network with high frequency of OSPF link flaps, OSPF LSA purges.	
Recovery: Restart/switchover of the Management Module is the only recovery mechanism. This may result in temporary disruption of traffic. However, if the operator observes a low memory situation then the operator can check for the third condition mentioned in customer symptoms. If it is confirmed that it is a TE-LSA-Id high memory utilization and memory allocation fails are not seen yet then, At maintenance window, 1. Note down the current configuration of traffic engineering under mpls policy 2. un-configure MPLS policy mode OSPF traffic engineering completely as per below command. BROCADE(config-mpls-policy)#no traffic-engineering ospf Make sure that the TE data base is cleared using 'show mpls te database' 3. Configure OSPF Traffic engineering again using step 1 noted configuration. Above steps shall release all non-freed memory held by TE-LSA-Id entry in MPLS.	

Defect ID: DEFECT000605113	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: While adding OpenFlow rule with output port and queue, reloading the linecard can see unexpected software exception in Linecard.	
Condition: Adding OpenFlow rule with output port and queue, and reload the line card	

Defect ID: DEFECT000605297	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Parse error due to missing double quotes in two lines in MIB file. 1) --#TYPE "Brocade Trap: Lockup and recovery threshold exceeded 2) -- Destination %s SPI %s Message Type %u.	
Condition: MIB Compile errors seen due to parsing issues in certain SNMP Managers.	

Defect ID: DEFECT000605322	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: Management module resets when "show optic" command is issued immediately after inserting 100G QSP28 optic module into the CFP2 to QSFP28 adapter.	
Condition: Only if the CFP2 to QSFP28 adapter is in port 1 and port 2 has an optical module present.	

Defect ID: DEFECT000605338	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: Port speed seen at controller was incorrect in the following scenario 1. Upon reload 2. OpenFlow is enabled when port admin state is 'Disabled'	
Condition: 1. Reload 2. OpenFlow enabled when port admin state is disabled	
Workaround: Remove and re-add OpenFlow configuration	

Defect ID: DEFECT000605694	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 06.0.00	**Technology:** LAG - Link Aggregation Group
Symptom: LAG's primary port automatically changes to a new port when some member's port are deleted from the LAG.	
Condition: When a group of ports are deleted from a LAG, and if the primary port does not belong to the group of ports deleted, then the primary port of the LAG changes. This issue will occur when dynamic LAG primary port feature is configured.	

Defect ID: DEFECT000605720	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Software forwarded packets (like fragmented packets, TCP SYN packets in the presence of TCP MSS adjust configuration) go to the wrong port leading to traffic loss.	
Condition: In a MCT topology, after ARP/MAC movement happens from ICL to another physical port.	
Recovery: "clear ip route" for the affected traffic.	

Defect ID: DEFECT000605728	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** BGP4+ - IPv6 Border Gateway Protocol
Symptom: Available system memory depletes steadily and conditions may be seen such as the inability to establish new SSH sessions.	
Condition: BGP has to be configured and it receives erroneous/badly constructed update messages from its peer.	
Recovery: If available memory continues to deplete and hits a very low level (<10%), switch over to standby Management module (when available) OR reloading the Management module can help temporarily.	

Defect ID: DEFECT000605788	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Management module may hit an exception and may undergo reload on continuous enable/disable of PCEP using '[no] router pcep'.	
Condition: While SNMP walk on PCEP MIB is underway, repeatedly unconfigure and configure PCEP router using "[no] router pcep" command	
Recovery: Reload the router after management module exception if auto reload is disabled.	

Defect ID: DEFECT000606368	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Ports configured under GTP profile is lost from running configuration upon reload.	
Condition: When a LAG port is added to the GTP profile and if the corresponding LAG has individual ports (non-consecutive) only or has a combination of individual (non-consecutive) as well as range of ports configured. Following is the example configuration with non-consecutive ports that gets lost on reload, gtp brc_gtp_profile_strip_lag 1 ports eth 14/1 eth 14/3 eth 32/4 ingress-inner-filter Following is the example configuration with non-consecutive ports as well as range of ports, that gets lost on reload, gtp brc_gtp_profile_strip_lag 1 ports eth 14/1 to 14/5 eth 32/4 ingress-inner-filter	

Defect ID: DEFECT000606395	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.9.00	**Technology:** MPLS Traffic Engineering
Symptom: Management module will unexpectedly reset	
Condition: This will happen only when "mpls adjust-bandwidth lsp <name>" is entered with a name other than one of the configured non-bypass RSVP LSPs on that system.	
Workaround: It can be avoided by ensuring that the entered name is correct and of an already configured non-bypass RSVP LSP on the system.	

Defect ID: DEFECT000606557	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: Line card may reload while handling BFD session creation	
Condition: This issue is observed when creating BFD over trunk. It could occur if trunk goes DOWN or flaps during BFD session initiation. This may occur when BFD session are getting created.	

Defect ID: DEFECT000607543	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Software Installation & Upgrade
Symptom: "cu_get_one_port_gig_type_from_lp(): mplp_show_send_request_to_lp() failed (2)" error thrown during MBRIDGE image sync to standby MP while performing simplified upgrade. No impact on simplified upgrade and it completes successfully.	
Condition: Performing simplified upgrade. Conditions are not definite.	

Defect ID: DEFECT000607574	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** CLI - Command Line Interface
Symptom: MBRIDGE upgrade progress message as shown below might get delayed Copy to MBRIDGE PROM.....Save the new MBRIDGE to flash.....Done Copy MBRIDGE IMAGE to standby MP, please wait.	
Condition: During MBRIDGE upgrade copying from Compact Flash.	

Defect ID: DEFECT000607624	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** ARP - Address Resolution Protocol
Symptom: Traffic is not forwarded to directly connected host when traffic is received for the host from 2 different VRFs.	
Condition: Connected routes leaked from one VRF to another VRF	

Defect ID: DEFECT000608460	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: (S,G) entry is not created in "show ip pim mcache" with RACL configured on CES/CER	
Condition: On CES/CER when RACL is configured with explicit IGMP permit ACL like below: access-list X sequence Y permit igmp a.b.c.d 0.0.0.255 any Note: This is specific to CES/CER only.	
Workaround: Explicitly permit all IP traffic from the source subnet to the multicast group address for the (S,G) to be created. For example: access-list x sequence y permit ip a.b.c.d 0.0.0.31 host e.f.g.h	

Defect ID: DEFECT000608572	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: During SNMP polling of 100Gx2-CFP2 optics OR the CFP2 to QSFP28 adapter, the Management module may unexpectedly reload and switch over to the standby Management module if available.	
Condition: SNMP polling on tables: “snIfOpticalMonitoringInfoTable” OR “snIfOpticalLaneMonitoringTable" with 100Gx2-CFP2 optics OR CFP2 to QSFP28 adapter.	
Workaround: Disable SNMP polling for the tables: “snIfOpticalMonitoringInfoTable” and “snIfOpticalLaneMonitoringTable".	

Defect ID: DEFECT000608991	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** IPv4 Multicast Routing
Symptom: Some of the multicast streams stopped working.	
Condition: Primary LAG port in OIF is down and traffic is reaching the node after the (*,G) entry is created.	
Workaround: Bring primary LAG port up.	
Recovery: clear ip pim mcache where LP receives traffic but does not create (S,G) entry	

Defect ID: DEFECT000609090	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: Static secured MAC addresses are flushed on a PMS enabled port while disabling the same port.	
Condition: PMS configuration should be enabled on port. Static MAC address should be configured. Disable the PMS enabled port.	

Defect ID: DEFECT000609387	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** ARP - Address Resolution Protocol
Symptom: Unable to add static ARP entries with an error message, "ARP: Errno(6) Number of Static ARP entries has exceeded the max limit".	
Condition: The router acts as a DHCP relay agent and it receives DHCP packets with options. DAI table is full	

Defect ID: DEFECT000609876	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: When BFD is used over VE interface across a layer 2 port, PCP value is incorrect. This value should be 7, but it is marked with 0. This issue will occur if PBIF (Hardware TX assist) is enabled and could be seen after BFD session state is UP.	
Condition: PCP value will be 0 in the BFD packet after the BFD session state is UP.	

Defect ID: DEFECT000610054	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Some traffic over IPSEC tunnel may be dropped	
Condition: When the router needs to further fragment already fragmented IP packets to send over IPSEC tunnel. The fragmentation ID and offset in the new IP fragments are not set correctly, rendering the end device unable to reassemble the packets.	
Workaround: Configure the IP MTU of the upstream device to match the IP MTU of the IPSEC tunnel, or use Path MTU Discovery to ensure that fragmented packets coming into the router are not further fragmented.	

Defect ID: DEFECT000610277	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** HTTP/HTTPS
Symptom: Management Module may unexpectedly reload (and switches over to the standby Management Module if available). The following stack trace will be seen: - Possible Stack Trace (function call return address list) 2243d048: memcpy(pc) 209ae9e4: A1RecordCrypt(lr) 209adf34: A1RecordProcess 209a928c: A1ConnectionDispatch 209af994: SsiReceiveStatus 2097ab68: AsCheckTcpReceiveStatus 2097a598: HandleWaitingForReceive 20979c14: HandleConnectionTask 209799b4: AllegroMainTask 20990084: http_web_agent 20990b70: http_timer_callback 20b556f4: itc_process_msgs_internal 20b55ba0: itc_process_msgs 209911f4: web_task 00005e18: sys_end_task	
Condition: Continuous data transfer through HTTPS connection.	

Defect ID: DEFECT000610601	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: MP module resets due to accessing an invalid memory. Issue was seen when having a "100Gx2-CFP2 2-port 100GbE Module" module with the optic type "100GE QSFP28" in the first port and poll for any of the following SNMP tables. o snIfOpticalMonitoringInfoTable o snIfOpticalLaneMonitoringTable	
Condition: The issue was seen when having a "100Gx2-CFP2 2-port 100GbE Module" module with the optic type "100GE QSFP28" in the first port and second port can have either CFP2 or QSFP28 optic and and poll for any of the following SNMP tables. o snIfOpticalMonitoringInfoTable o snIfOpticalLaneMonitoringTable	
Workaround: If possible try to exclude the SNMP tables (snIfOpticalMonitoringInfoTable, snIfOpticalLaneMonitoringTable) from polling.	

Defect ID: DEFECT000610730	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Configuration Fundamentals
Symptom: Port flaps will be observed 3-4 times when 100G CFP2 SR10 or QSFP28 port is enabled.	
Condition: Always	

Defect ID: DEFECT000610776	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.8.00	**Technology:** MPLS Traffic Engineering
Symptom: In a network with MPLS RSVP LSP with FRR configured, detour won't come up at PLR	
Condition: Merge point router's outgoing interface has admin group configured which is excluded in FRR configurations under LSP	

Defect ID: DEFECT000610820	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: Link flaps 3 or 4 times before the link stays UP when disabling and enabling an interface having CFP2 SR10 or QSFP28 transceiver modules.	
Condition: This issue is specific to QSFP28 and CFP2 SR10.	

Defect ID: DEFECT000610993	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** IPv6 Addressing
Symptom: Router will experience elevated CPU usage on the management module which may hamper its normal operation.	
Condition: Reception of IPv6 ND6 packets with Hop Limit set as 255.	
Workaround: On GEN3 module, apply User Defined ACL (UDA) to filter out invalid ND6 packets in the hardware with software release 5.9 or later.	

Defect ID: DEFECT000611054	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.4.00	**Technology:** Syslog
Symptom: On occasion, optic on 24x1G Linecard module type may cause i2c bus lockup on the Linecard resulting in very frequent error messages similar to the SYSLOG entries seen below: E:System: Can't read LP6 PCB temperature! E:System: Can't read LP6 XPP temperature!	
Condition: Usage of third party optic or any bad optic on 24x1G Linecard module.	
Recovery: "show media" command could help recover from the condition for a short interval. The recovery could last for days, depending on the load on i2c bus.	

Defect ID: DEFECT000611080	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: Port with QSFP28 optic module is not coming up after a series of plug-out/plug-in.	
Condition: Applicable to QSFP28 optic module in CFP2 to QSFP28 port.	

Defect ID: DEFECT000611357	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.7.00	**Technology:** IP over MPLS
Symptom: In a scaled network with several parallel TE links between pairs of RSVP routers and a large number of TE nodes and links, some LSPs might not come up due to a "loop detected" error. Warning message "Warning: Infinite Loop in mpls_cspf.c:3769: mpls_constrained_dijkstra 4" will be seen on the router. LSP's CSPF computation will fail and some LSPs may stay in down state due to "loop detected" CSPF error. Up LSPs will not be impacted; only the newly coming up LSPs might stay in a down state.	
Condition: This issue will been seen only in a large MPLS/RSVP network with tens of TE nodes and hundreds of links + parallel links between pairs of TE nodes.	
Workaround: There is no "non-intrusive" workaround. Removing parallel links from the topology will help.	
Recovery: No easy recovery other than reducing the number of parallel links.	

Defect ID: DEFECT000612208	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** sFlow
Symptom: Error message related to sFlow configuration is displayed with incorrect Primary port number in the CLI when a new member port is added in an already deployed LAG.	
Condition: This happens in the following cases: - - When the Primary port in a deployed LAG is already configured with sFlow and the member port to be added newly in the LAG does not have sFlow configured. - When the LAG ports in the deployed LAG do not have a sFlow configuration but the member ports to be added in the LAG have a sFlow configuration.	
Workaround: Ensure that the configuration on the new port is the same as the configuration on the LAG.	

Defect ID: DEFECT000612383	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: First packet to directly connected host is dropped after GRE tunnel termination.	
Condition: L3 forwarding to directly connected host after GRE termination. IP route for interface subnet route programmed to trap and no host entry is programed in HW.	

Defect ID: DEFECT000612475	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.1.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP polling for QSFP28 optics data returns Unsupported data.	
Condition: SNMP Polling for QSFP28 optics data on 2x100G-CFP2 line card module.	

Defect ID: DEFECT000612750	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** ACLs - Access Control Lists
Symptom: Error message (error - H4) is getting displayed during reload. Sample output is given below: - Router#reload Checking for coherence... Done. Are you sure? (enter 'y' or 'n'): y Halt and reboot NetIron XMR/MLX Boot Code Version 5.9.0 ///// OUTPUT TRUNCATED ///// system memory: 4294967295, available 3506524160 FID manager initialized ... Start init runconfig from start config Load config data from flash memory... error - H4	
Condition: No ACL is bound to any interface on the device, "force-delete-bound-acl" is enabled and the device is reloaded. Note: This issue is applicable across all releases. The error message displayed is an indication of the condition of no ACLs bound to any interface and does not have any impact on the system.	
Workaround: Avoid using "force-delete-bound-acl" command option when no ACL is bound to any interface on the device	

Defect ID: DEFECT000613063	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** IP Source Guard
Symptom: RPF loose mode doesn't work. Packets are routed instead of dropping when there is no valid source route.	
Condition: "sflow null0-sampling" is configured with RPF loose mode.	

Defect ID: DEFECT000613729	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: 100Gx2-CFP2 line card may reload unexpectedly with the following stack trace:- 20bb3178: mod_rw2x100_g3_cfp2_reset_steps(pc) 20bb3170: mod_rw2x100_g3_cfp2_reset_steps(lr) 2002d8cc: cfp_reset 209b4fe0: phy_conn_enable 20a2fb2c: port_check_port_status 20a339a8: port_link_status_poll 20a334ac: port_status_poll 200058c0: perform_callback 200062c8: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f2ec8: main 00040158: sys_end_task	
Condition: Continuous Optic Insertion and Removal is done for 100G LR4 CFP2 optics multiple times	

Defect ID: DEFECT000614029	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** IPv6 Addressing
Symptom: Appropriate error message is not printed on console when user configures IPv6 tunnel interface as MPLS interface.	
Condition: Configuring IPv6 tunnel interface as MPLS interface is not supported. Appropriate error message was not printed on console when user configured IPv6 tunnel interface as MPLS interface.	

Defect ID: DEFECT000614112	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: OSPFv2 Type-3 summary LSA originated for area-range configuration is not flushed (withdrawn) even if all the component routes that fall within the area-range are removed.	
Condition: (1) area-range command on ABR is configured (2) component routes that fall within the range are in RTM (e.g., configure some IP interfaces with addresses that fall within the range) (3) disabling all the component routes (i.e., disable the configured interfaces with IP addresses that fall within the area-range).	
Workaround: If the ABR status is made to loose then it would flush (withdraw) the area-range summary.	

Defect ID: DEFECT000614508	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: "show ip ospf data link-state extensive" does not display extensive output of all LSAs.	
Condition: At least 8 Loopback interfaces advertised to the peer. Multiple entries of router LSAs in the OSPF database.	

Defect ID: DEFECT000615179	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP community configuration have duplicate entry in "show running"	
Condition: When SNMP community is configured with ACL name like below: snmp-server community public ro <acl-name>	

Defect ID: DEFECT000615868	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** VLAN - Virtual LAN
Symptom: Traffic rate limited to 20Gbps for all VLANs where outbound the rate-limit is not applied.	
Condition: 1) This is specific to MLX-10Gx24. 2) Outbound rate-limit is applied on one specific VLAN.	
Recovery: Only recovery is to reload the corresponding line card module after applying the rate-limit to the configuration.	

Defect ID: DEFECT000615906	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP polling for IPSEC tunnel interfaces doesn't provide correct values	
Condition: When polling for IPSEC tunnel interface statistics through SNMP table IfTable.	
Workaround: Execute the CLI command "show interface tunnel <tunnel-id>" before polling SNMP table IfTable.	

Defect ID: DEFECT000615910	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Telemetry
Symptom: SNMP polling of ifTable statistics always displays the value as zero for MPLS LSP tunnel	
Condition: When polling MPLS LSP statistics through SNMP table ifTable.	

Defect ID: DEFECT000616566	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Configuration Fundamentals
Symptom: Management module hit a software exception and will reload when user pastes the self-signed certificate with invalid time range	
Condition: The SW exception occurs when user pastes the self-signed certificate on terminal with not a valid time range. This should be avoided, as entering invalid certificates is not needed in customer environment.	

Defect ID: DEFECT000616823	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Sysmon
Symptom: CES/CER may unexpectedly reload with the following stack trace :- Possible Stack Trace (function call return address list) 203056d0: hashFastGenericGet(pc) 209e748c: itc_registry_get_msg_def_for_msg_type(lr) 209e748c: itc_registry_get_msg_def_for_msg_type 209dfbf0: validate_params_and_get_msg_def 209dfc98: itc_send_request 20a0e608: CancelTimerCommon 20a0e788: CancelTimer2 209b9dbc: ssh_close_connection 209b1a00: cu_ssh_close_session_internal 209b3a90: ssh_cu_msg_callback 209e0954: itc_process_msgs_internal 209e0df4: itc_process_msgs 207179f0: snms_task 00040158: sys_end_task	
Condition: There is no known condition/trigger for this issue. Note: This is specific to CES/CER only.	

Defect ID: DEFECT000617836	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Linecards on an MLX unexpectedly reloading at random intervals. The stack trace seen using the "show save" command is as follows - 212c0860: ipcom_pqueue_get_next(pc) 212ca014: ipcom_tmo2_select(lr) 21204e70: ike_wr_timer 211e874c: ike_sys_timer 00040160: sys_end_entry 0005e4c8: suspend 00062230: receive_message 00005024: xsyscall 211e8c28: ike_task 00040158: sys_end_task	
Condition: Can be seen on all MLX Line Cards running NetIron 5.8.00 through 5.8.00e, 5.9.00 through 5.9.00bd, 6.0.00 and 6.0.00a images. Can be caused by IPSec control packets.	

Defect ID: DEFECT000618044	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: LP unexpectedly reloads with the following info seen in "show save" in function is_routemap_in_use_by_uda_pbr()	
Condition: Can be seen - during LP bootup, OR - when an IP or UDA route-map is configured.	

Defect ID: DEFECT000618076	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 06.0.00	**Technology:** Traffic Queueing and Scheduling
Symptom: Linecard module may unexpectedly reload with the following stack trace: - Possible Stack Trace (function call return address list) 2064de14: rw2_petra_set_port_rate(pc) 2064ddf8: rw2_petra_set_port_rate(lr) 2119c424: fdry_tm_set_port_rate 20ff40c8: lp_tm_offload_handler 207f3a2c: lp_tm_offload_task 00040158: sys_end_task	
Condition: When the linecard module comes up and the remote ports connected to the local ports are flapping	

Defect ID: DEFECT000618134	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** High Availability
Symptom: Standby management module went down with the syslog ‘reason None. Error Code 0’ and no error log dump. SYSLOG: <13>Sep 20 15:15:55 System: Standby Management Module was down, reason None. Error Code 0.	
Condition: On terminating the Telnet/SSH session immediately after issuing ‘write mem’ command.	
Workaround: Wait for 2-3 sec before killing the telnet session after issuing ‘write mem '. Note: The issue will not affect traffic as it is a Standby module and comes back in a few minutes.	

Defect ID: DEFECT000618333	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: TCP packets are received in the server without removing the GRE header.	
Condition: When trying to telnet to the Linux host from a server with a GRE tunnel between and with TCP MSS configured in the transit MLX device.	
Workaround: The configuration "ip tcp adjust-mss" has to be removed.	

Defect ID: DEFECT000618580	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** SSH - Secure Shell
Symptom: Unable to upload SSH client-pub-key file due to size-limit.	
Condition: When uploading the SSH client-pub-key file with the size of more than 4096 bytes.	

Defect ID: DEFECT000618928	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** ACLs - Access Control Lists
Symptom: Newly added LAG port is in LACP blocked state	
Condition: Apply a MAC ACL on a port and create LAG with this port. Remove the ACL and add another ACL. Now add a secondary port to the LAG from another LP	

Defect ID: DEFECT000619510	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** VLAN - Virtual LAN
Symptom: RSTP configuration is not allowed under vlan-group and Error message is displayed as "spanning tree configuration is enabled".	
Condition: 1) "Spanning tree" command is globally configured 2) configure "rstp" command under vlan-group having member vlans.	
Workaround: Remove the spanning tree configuration from each vlan under vlan-group and configure rstp.	

Defect ID: DEFECT000619879	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 06.1.00	**Technology:** Rate Limiting and Shaping
Symptom: Access-list accounting output displays accounting even if "enable-accounting" isn't configured in the rule.	
Condition: This can be seen when the command to display access-list accounting for ACL based rate-limiting bindings is executed by user.	

Defect ID: DEFECT000619934	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: Memory leak may be observed during execution of either of the following commands: 1) ‘show rate-limit interface x/y output’ 2) 'show sysmon events brief'.	
Condition: 1) The command ‘show rate-limit interface x/y output’ may result in a memory leak when rate-limit is not configured 2) The command "show sysmon events brief' may result in memory leak when sysmon events are not configured	

Defect ID: DEFECT000620066	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: "snmp-server group" configuration is lost after the reload.	
Condition: "snmp-server group" name configured and reload the device.	

Defect ID: DEFECT000620729	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv4 Multicast Routing
Symptom: "pim-sparse" configuration getting lost on the GRE Interface after chassis Reload and could lead to a multicast data traffic loss issue.	
Condition: "pim-sparse" configuration on GRE interface.	
Workaround: Post reload of the device, configure pim-sp manually on gre-tunnel interface again.	

Defect ID: DEFECT000620803	
Technical Severity: High	**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: Enable ISIS for IPv6 with multi-topology transition and then run 'show IPv6 route', shortly after this CER reloaded unexpectedly with the following stack trace:- 20e57ec4: bgp_best_route_selection_with_sorting(pc) 20e57dbc: bgp_best_route_selection_with_sorting(lr) 20e582c8: bgp_best_route_selection_and_change 20f05a68: bgp_check_and_update_bgp_route_in_ip_table_as_necessary 20e77790: bgp_route_damping_timer_event 20f221f8: bgp_timer 20f1d780: bgp_timeout_func 20a47fe8: itc_process_msgs_internal 20a48494: itc_process_msgs 20ec0768: bgp_task 00040158: sys_end_task	
Condition: CER reload is observed when BGP Best path flaps. BGP best path can flap in scenarios for example lBGP next-hop change, flapping BGP route etc..	

Defect ID: DEFECT000621666	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: Management Module may unexpectedly reload and switch over to the standby Management Module if available. The following stack trace will be seen: - Possible Stack Trace (function call return address list) 20ef84a4: ospf_router_receive_packet_callback(pc) 20ef849c: ospf_router_receive_packet_callback(lr) 20a1c040: itc_process_msgs_internal 20a1c380: itc_process_msgs 20ef775c: ospf_msg_task 00005e18: sys_end_task	
Condition: After running for longer duration. Low memory available in OSPF memory pool.	

Defect ID: DEFECT000622131	
Technical Severity: High	**Probability:** High
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: On a Customer-Edge router if external LSA's tag matches OSPF domain-tag then these external LSA's would not be installed in OSPF route table.	
Condition: In VRF-lite case if a Customer-Edge router is running OSPF in a VRF, and if external LSA contains tag same as OSPF domain-tag then these external LSAs would be missing in route table.	
Workaround: On Customer-Edge router configure OSPF domain-id different than the one present in OSPF external LSA tag.	

Defect ID: DEFECT000622744	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: Line card module may unexpectedly reload and get into a continuous reload cycle with the following stack trace:- Possible Stack Trace (function call return address list) 210ba9b8: sw_l4_find_acl_table(pc) 210306d0: sw_l4_construct_port_list_for_rule_based_acl(lr) 21030a6c: sw_l4_construct_acl_rule_mask_and_prog_cam 2103154c: sw_l4_update_acl_cam_entries 21039d30: l4_update_rule_based_entries_in_cam 2103199c: l4_lp_inbound_acl_update_timer_callback 200058c0: perform_callback 200062c8: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f2f88: main 00040158: sys_end_task	
Condition: 4K VEs associated one on one with 4K VLANs. (VE 2 to VE 4095) One physical port part of all the 4K VLANs. 4K IPv4 ACL having 25 rules per ACL. These 4K different ACLs are bound on the 4K VEs	

Defect ID: DEFECT000623145	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: When OpenFlow rule is configured with L2VPN, the packets that come out of the MPLS network are deformed as invalid packets.	
Condition: Enable OpenFlow on MPLS LSP. Configure OpenFlow rule with LSP and L2VPN label in action. In the MPLS egress encounter, the packets are getting dropped.	

Defect ID: DEFECT000623395	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: After line card reload, Traffic is not rate limited based on L2 ACL on secondary LAG member ports.	
Condition: Bind a L2 ACL rate-limit on a multi slot LAG with primary and secondary ports in different slot and then reboot the line Card which has secondary port of LAG.	

Defect ID: DEFECT000623430	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: High cpu utilization on 8x10G linecard module.	
Condition: Rarely a port on 8x10G module can get into PHY lockup. If this lockup state is continuous, CPU utilization can go higher.	
Recovery: Disable the affected port from configuration to bring the CPU usage down.	

Defect ID: DEFECT000623554	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: Even if the user saves the changes in the 'fan-threshold' configuration, those are not applied after reload or switchover. Users will also see the error related to invalid input while the system boots. For example, 'Invalid input -> med 65 80 med-hi 73 90 hi 75 105, fan-threshold lp-tcam low 68 med 65 80 med-hi 73 90 hi 75 105'	
Condition: When user does some changes in the configuration pertaining to 'fan-threshold', saves the changes and reload or switchover.	
Recovery: Remove the config related to 'fan-threshold' and save the config.	

Defect ID: DEFECT000623841	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: Management Module may unexpectedly reload (and switches over to the standby Management Module if available). The following stack trace will be seen: - Possible Stack Trace (function call return address list) 20fd7150: bgp_prepare_nlri_holder(pc) 20fd5e5c: bgp_best_route_selection_with_sorting(lr) 20fd5e5c: bgp_best_route_selection_with_sorting 20fd6574: bgp_best_route_selection_and_change 20fa6c94: bgp_check_and_update_bgp_route_in_ip_table_as_necessary 20fa63a8: bgp_add_bgp_routes_to_routing_table_if_necessary_callback 210336ec: bgp_tree_partial_traverse_with_possible_change 20fa67cc: bgp_add_bgp_routes_to_routing_table_if_necessary 20fb4764: bgp_check_updates 20fc1420: bgp_timer 20fc1050: bgp_timeout_func 20b92d10: itc_process_msgs_internal 20b931bc: itc_process_msgs 21015b80: bgp_task 00005e18: sys_end_task	
Condition: Management Module may unexpectedly reload when BGP Best path flaps. BGP best path can flap in scenarios like lBGP next-hop change, flapping BGP route etc..	

Defect ID: DEFECT000624544	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** Hardware Monitoring
Symptom: CES/CER may unexpectedly reload with the following stack trace :- Possible Stack Trace (function call return address list) 21ff3114: memset(pc) 2037c4ac: os_malloc_zero(lr) 2097b280: mplp_send_itc_response 2097bf40: mplp_process_lp_data_response_continue 2095579c: itc_continue_deferred_response 2097c61c: mplp_process_lp_data_response 20954920: itc_process_msgs_internal 20954c58: itc_process_msgs 2097e408: lp_agent_task 00040158: sys_end_task	
Condition: There is no known condition for this issue to occur.	

Defect ID: DEFECT000625221	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.1.00	**Technology:** HTTP/HTTPS
Symptom: This Defect is created as per CVE-2016-2183: The DES, and Triple-DES ciphers susceptible to "Sweet32" attack. (Birthday bound of approx 4 billion blocks)	
Condition: This Defect is created as per CVE-2016-2183: The DES, and Triple-DES ciphers susceptible to "Sweet32" attack. (Birthday bound of approx 4 billion blocks).	
Workaround: Do not use DES, or Triple-DES ciphers from a Web Browser.	
Recovery: Do not use DES, or Triple-DES ciphers from a Web Browser.	

Defect ID: DEFECT000626658	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.8.00	**Technology:** IPv4 Multicast Routing
Symptom: Router may experience intermittent ICL link instability and reload unexpectedly with the following stack trace:- 2034e390: pim_remove_oif_from_entry 21db84e8: pim_assert_update_oif_state 21db9544: pim_assert_cleanup_state 21db9304: pim_assert_cancel_assert 21db8798: pimsm_assert_run_fsm 2034d280: pim_add_oif_to_entry 21d266ac: mcast_mct_process_ingress_change 20352b7c: mcast_set_parent_phy_port 21da0794: pimsm_l2reg_update_phy_port_from_arp 21da0d1c: pim_process_register_msg 21daff90: mcast_receive_slave_message_internal 21daeb90: mcast_receive_slave_message 209f040c: itc_process_msgs_internal 209f08ac: itc_process_msgs 21d23378: mcast_task 00040158: sys_end_task	
Condition: When PIM ASSERT Winner OIF moves to blocked state.	

Defect ID: DEFECT000627973	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** IPv6 Addressing
Symptom: CAM violation syslog message is generated along with invalid entry error message on line card console.	
Condition: Only on line cards with algorithmic mode, while an already existing IPv6 route entry is getting added repeatedly (duplicate entry). This results in a CAM violation syslog message.	

Closed without code changes

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as 12/19/2016 in R06.1.00.

Defect ID: DEFECT000562915	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast Routing
Symptom: Transient multicast traffic loss during first time switchover	
Condition: Traffic loss is seen only when first time failover happens.	

Defect ID: DEFECT000579677	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.7.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: In some rare situation, incorrect MAC learning causes reach-ability issues on a CES/CER.	
Condition: Remote MAC learned under a wrong VPLS instance.	

Defect ID: DEFECT000580123	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
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: Under rare circumstances, multiple switch over of Management module done back to back, could result in some of the BGP sessions flapping once or twice	
Condition: Multiple switch over of the Management Module done back to back on a router that has configuration of the following scale: - - 100+ IBGP neighbors - 100+ EBGP neighbors	

Defect ID: DEFECT000580784	**Technical Severity:** High
Reason Code: Design Limitation	**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: Multiple time sensitive protocols like VRRP, BFD flap observed for short duration on a CES/R device.	
Condition: BGP flap on a CES/CER device with following scale of configuration: - Number of BGP peers: More than 50 Number of routes installed in BGP database: close to one million Number of routes in RTM: more than 500000 Number of VRRP router instances: more than 200 Number of OSPF neighbors : 10 or above Number of BFD sessions: 5 or above Note: This is applicable only for CES/R platform	

Defect ID: DEFECT000588040	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Reload of devices in a MCT/VPLS network within 5-10 minute of each other may lead to MCT VPLS traffic loss	
Condition: Reload of devices with MCT VPLS configuration.	

Defect ID: DEFECT000588168	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** ICMP - Internet Control Message Protocol
Symptom: While doing ping to local IP on the router, latency of more than 10msec seen.	
Condition: When ICMP packets are processed in the CPU, a latency introduced when there are ARP updates in the system/network.	

Defect ID: DEFECT000590226	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.7.00	**Technology:** Rate Limiting and Shaping
Symptom: All packets ingressing on one tower on an LP are dropped. "show np statistics" shows the "NP Rx Priority 0/1 Drop" counter incrementing.	
Condition: Seen on 20x10G, 2x100G-CFP2 and 4x40G modules, when ACL rate limiting has been configured and ACL rebinding is happening frequently. The issue was seen after 15 days when ACL rebinding was happening every 2 hours. If rebinding happens more frequently, the issue is likely to happen within a shorter duration.	

Defect ID: DEFECT000591513	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** IS-IS - IPv4 Intermediate System to Intermediate System
Symptom: IS-IS peer node reachability may be shown as multihop although it is a single hop	
Condition: This issue may be observed in a scaled IS-IS topology with shortcuts enabled	

Defect ID: DEFECT000591587	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast Routing
Symptom: Multicast software cache entries are not deleted after entries are aged out from hardware in an MCT network.	
Condition: This issue has introduced after stopping multicast source traffic.	
Recovery: System can be recovered from this state by clearing cache entries using "clear ip pim mcache" command.	

Defect ID: DEFECT000592787	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: LP module may hit an exception and is reset by the MP - after that about 80% of Local VPLS traffic is TM dropped - does not recover	
Condition: Line card reset post an exception may cause such conditions where 80% of the local VPLS traffic will be dropped at TM	

Defect ID: DEFECT000593492	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv4 Multicast Routing
Symptom: Sometimes device may reload when user undeploy and deploy LAG interface after some specific configuration steps along with the Multicast traffic in an MCT deployment.	
Condition: This issue introduced when user un-deploy and deploy LAG interface after some specific configuration steps along with the Multicast traffic in an MCT deployment.	
Workaround: Stop Multicast traffic and clear cache entries before un-deploy and deploy of the LAG in an MCT deployment.	

Defect ID: DEFECT000594173	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** High Availability
Symptom: The customer at the time of issuing a reload on the system might see the below error/warning if the setup is loaded and scaled. Warn:alloc_and_distribute_base_fid: Sync to standby MP failed for FID 0 (0000) (err = Timeout), reboot it(g_mp_red_wait_done 0). In this case, setup was considerably scaled setup having 4k Vlans, 128 RTSP sessions, llldp enabled, LCP, etc	
Condition: On a scaled setup the sync may not complete in time and result in timeout thereby causing the messages to be printed. The sync is required to maintain the correct states across active and standby MP. At the time of reload the sync couldn't complete in time due to load on the MP's and the IPC. Since this happens at reload the warning in itself is harmless and causes no functionality impact.	
Workaround: No workaround	
Recovery: The system just reloads fine without any functional impact	

Defect ID: DEFECT000594318	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** SSH - Secure Shell
Symptom: The SSH session terminates unexpectedly when running "show tech- support" command.	
Condition: From an SSH session, execute "show tech-support" command on a scaled setup with large configuration (32 slot chassis with ACL configurations close to the supported maximum limit).	
Workaround: Redirect the output of "show tech-support" to a file instead of streaming to the SSH terminal. Example: abc@xyz{295}: ssh lab@w.x.y.z > show_tech_l2.txt Password: <<<< Provide password here, and monitor the output in a separate window (see below) <<<< Now we are at user privilege level prompt. So enter "enable" <<<< Now we are at privilege exec mode. So enter "show tech" <<<< wait for output to complete. Then exit twice (for exit out of privilege mode, and then exit out of user mode) Connection to w.x.y.z closed by remote host. Connection to w.x.y.z closed. abc@xyz{296}: In a separate window the output can be monitored as follows: - abc	

Defect ID: DEFECT000595623	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv4 Multicast Routing
Symptom: Line-card may reload while running multicast data traffic in an unlikely user scenario.	
Condition: Trigger for this issue is unknown. Should not occur under normal maintenance operation, represents an unlikely user scenario. This system has IPSEC Tunnels with PIM enabled.	

Defect ID: DEFECT000596126	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
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: Router restart is observed.	
Condition: This sometime occurs if clearing of all BGP and OSPF neighbors is performed just after the switch-over to standby MP.	

Defect ID: DEFECT000596167	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** PBR - Policy-Based Routing
Symptom: After reload PBR counters are not getting updated on CES devices.	
Condition: This happens only in reload scenario.	
Recovery: Rebind the PBR.	

Defect ID: DEFECT000596272	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** IP Addressing
Symptom: Unable to ping a small number of IPs (including some directly connected IPs).	
Condition: On CER/CES platform, with high number (100s) of directly connected hosts with multiple non-major subnets	

Defect ID: DEFECT000596289	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Telemetry
Symptom: No able to clear ACL/PBR counters using command "clear access-list ethertnet x/y"	
Condition: Clearing of counters not working	
Workaround: User can use "clear access-list ethertnet x/y policy-based-routing" for clearing PBR counters. And "clear access-list " for clearing acl counters	

Defect ID: DEFECT000597443	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS Traffic Engineering
Symptom: RSVP-TE LSP is operationally up from control plane point of view but is broken at the data plane. Data traffic passing through this LSP is affected.	
Condition: Line card on one of the transit routers through which LSP passes was continuously rebooting. After faulty line card was replaced, LSP cameup but it's data plane was broken.	
Recovery: Resetting the LSP resolved this issue. Execute the following commands conf t router mpls lsp <NAME> disable ==wait for around 1min== enable	

Defect ID: DEFECT000598427	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: "client-interface shutdown" command does not bring the CCP down and MCT VPLS Active/Standby switchover does not happen	
Condition: VPLS should be configured and "client-interface shutdown" command should be issued	

Defect ID: DEFECT000599114	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: When MCT VPLS cluster node status changes from Active to Standby, VPLS session between MCT and remote peer does not go down, and MAC address(es) learned against the VPLS session on the Remote peer are not flushed. This will result in traffic loss from the remote peer to the client devices.	
Condition: “client-interface shutdown” is enabled on MCT VPLS cluster.	
Recovery: Flap the remote peer OR execute "clear mac" on remote peer.	

Defect ID: DEFECT000599410	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: The "tunnel mtu" configuration under the GRE tunnel does not show up after system reload when the tunnel MTU is configured more than default GRE MTU (1476). Before reload: #sh run int tun 1 interface tunnel 1 tunnel mode gre ip tunnel mtu 1481 tunnel source a.b.c.d After reload: #sh run int tun 1 interface tunnel 1 tunnel mode gre ip tunnel source a.b.c.d Note: this is just a display issue and does not affect the functionality	
Condition: 1) Tunnel MTU value should be configured more than default GRE MTU (1476) under the GRE tunnel. 2) Save the configuration and reload the system.	
Workaround: Avoid setting the tunnel MTU to more than the default GRE MTU	

Defect ID: DEFECT000599909	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** LAG - Link Aggregation Group
Symptom: CFP2 100G port flaps several times on disable/enable of interface with UDLD configuration.	
Condition: Disable/enable the interface from link partner (with UDLD configured on both ends of the link).	

Defect ID: DEFECT000600401	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: When MCT CCP / VPLS goes up through chassis reload or MGMT module switchover etc, "log error- arguments specified does not match" message pops up always.	
Condition: MPLS LSP syslogs raised with wrong arguments	

Defect ID: DEFECT000600587	**Technical Severity:** Critical
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: Device/switch may reload due to an exception in SSL task while handling a bursts of Openflow msgs.	
Condition: Under heavy Openflow messages from Controller, the device/switch SSL connection to the Openflow controller may timeout, and the session may become invalid resulting in an invalid access causing the device to reload.	
Workaround: Reduce the rate of Openflow messages coming into the device/switch.	
Recovery: Reload the device/switch, if auto-reload is not enabled.	

Defect ID: DEFECT000602339	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** SSH - Secure Shell
Symptom: The device might suffer a reload while uploading a zero size file.	
Condition: When a zero length file is given as the file to be uploading for either SSL client certificate or private key, the device might suffer a reload due to invalid access.	
Workaround: Do not give a zero length file as the file to be uploaded for either SSL client certificate or private key file.	
Recovery: Reload the device, if auto-reload is disabled.	

Defect ID: DEFECT000603089	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: On a CES/CER device, traffic from non-PMS port is unicasted to PMS port and traffic from PMS port is flooded to all ports (both PMS and non-PMS) of the associated VLAN.	
Condition: This may happen when 1. Continuous bi-directional traffic is flowing towards PMS enabled port so that traffic is unicasted. 2. The same traffic stream is also received on the non-PMS port of the same device. Note: This issue is applicable only for CES/CER platform	

Defect ID: DEFECT000603774	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv6 Multicast Routing
Symptom: Multicast data traffic loss can happen for few IPV6 streams in a scaled multi-dimensional traffic on CES/CER device.	
Condition: With multiple reload and flapping of the port continuously and having scaled multidimensional traffic can lead to the traffic loss for some of the multicast stream for CES/CER device.	
Workaround: Avoid continuous reloading and flapping of ports for scaled traffic flow on CES/CER for multi-dimensional topology and traffics.	
Recovery: Clearing the affected mcache entry can help in recovering the traffic loss for affected stream.	

Defect ID: DEFECT000603798	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: "show media" command output shows "snSwIfInfoGigType" value as unknown for an optic in the slot.	
Condition: Performing below steps can put system into this state: 1. Simultaneous (atleast 3) SNMP polling for optics related SNMP tables. 2. Disable all the ports in the Linecard module 3. Power cycle the Linecard module.	
Recovery: Need to issue "show media" command in the corresponding Linecard module console.	

Defect ID: DEFECT000605003	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VLL - Virtual Leased Line
Symptom: Unexpected LP reload with MCT VPLS/VLL configuration.	
Condition: Neighbor router reload with MCT VPLS/VLL configuration may trigger this issue.	

Defect ID: DEFECT000623845	**Technical Severity:** Critical
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** Hardware Monitoring
Symptom: Linecard gets into rolling reboot when "sysmon spi crc-errors action reset-linecard' is enabled along with mirroring on one or more of its ports.	
Condition: The issue is seen when both mirroring (on one or more ports) and 'sysmon spi crc-errors action reset-linecard' are enabled. It is applicable to 1Gx48 and 10Gx8 modules and software versions NI 5.6.00hb and NI 5.6.00j only.	

Defect ID: DEFECT000623981	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** ARP - Address Resolution Protocol
Symptom: Directly connected host is not reachable from the upstream device.	
Condition: On CES/CER, when LPM NH recovery happened for host routes and when the default route has ECMP path.	

Defect ID: DEFECT000624821	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.7.00	**Technology:** MPLS Traffic Engineering
Symptom: RSVP component in MPLS hits a process exception when trying to FRR failover an LSP to its backup. Process exception for MPLS will result in reset of router's Management Module (MM) with eventual fail over to the standby MM if available. RSVP data traffic forwarding will suspend until standby MM is fully up (in dual MM case) or the MM resets and comes back up (in single MM case).	
Condition: For a Facility FRR LSP, when fault is detected on an unprotected link on the LSP's path, it will result in Fast Reroute at an upstream node. But since the failed link was not protected, Fast Reroute will not succeed and will result in an inconsistent state for the LSP that eventually leads to a process exception for MPLS/RSVP.	

Defect ID: DEFECT000626687	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Software Installation & Upgrade
Symptom: Line card module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20d9c878: clusterlp_catchall_program_timer(pc) 20d97260: clusterlp_ipc_cluster_set(lr) 20d97260: clusterlp_ipc_cluster_set 20c1a25c: ipc_multi_module_handler 207f378c: lp_assist_ipc_request_send 20c1c7a0: ipc_process_messages 20bcad68: ipc_process_rel_msg 20c1cf88: ipc_receive_packet 20036ce4: ge_process_ipc_data_msg 207f4814: lp_ipc_task 00040158: sys_end_task	
Condition: This issue is seen during hitless-reload	

Known issues

This section lists open software defects with Critical, High, and Medium Technical Severity as of 12/10/2016 in R06.1.00.

Defect ID: DEFECT000587202	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: Packet drops seen on ports due to Linecard module failing to process packets with error "RX Lookup unavailable"	
Condition: CAM FIFOs are stuck resulting in RX Lookup failure.	
Recovery: Reload the affected Linecard module	

Defect ID: DEFECT000587847	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Licensing
Symptom: Under rare conditions the device goes for unplanned restart after a switchover has happened.	
Condition: Likely scenario of reproduction when a switchover has happened and the systems been idle for some time post that. The conditions for reproducing the defect have not be known yet. This has been seen twice till now.	

Defect ID: DEFECT000600296	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: ARP packets are not sent to controller for flows which match on ether type ARP and with action as normal with controller action and mirror port	
Condition: Issue is seen when the flow does not match on a VLAN.	

Defect ID: DEFECT000602148	
Technical Severity: Medium	**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: DEFECT000602490	
Technical Severity: Medium	**Probability:** High
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: Incorrect Advertising router ID is shown in LSA database	
Condition: OSPFv2 is running with Multi-VRF and Inter-VRF config on CER	

Defect ID: DEFECT000602530	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 06.1.00	**Technology:** Rate Limiting and Shaping
Symptom: ARP packets are not rate-limited based on ARP rate-limit policy on 20x10G line card.	
Condition: Apply ARP rate limit policy globally after system reload.	
Workaround: Disable/Enable the ingress physical interface.	

Defect ID: DEFECT000603828	
Technical Severity: High	**Probability:** High
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: Very rarely router restart is observed if we issue "clear ipv6 ospf neighborship" in scaled topology.	
Condition: Invoking "clear ipv6 ospf neigborship" multiple times in OSPFv3 scaled topology.	

Defect ID: DEFECT000605799	
Technical Severity: High	**Probability:** Low
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: DEFECT000607620	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** SSH - Secure Shell
Symptom: In rare condition, system may disconnect SSH sessions unexpectedly due to a malformed header. The root cause is not yet known.	
Condition: In rare condition, system may disconnect SSH sessions unexpectedly due to a malformed header.	

Defect ID: DEFECT000607807	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.7.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP query timeout and queue full condition may be seen with 20x10 modules.	
Condition: High rate of optic data query through multiple SNMP pollers.	
Workaround: Reduce polling frequency of optic information.	

Defect ID: DEFECT000607934	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: OSPF protocol stays down as BUM traffic are not forwarded when received from VPLS peer	
Condition: MCT VPLS cluster configured traffic ingress through ICL/cluster-peer link from VPLS peer with "no vpls-cpu-protection" configured	
Workaround: Configure "vpls-cpu-protection" to forward all BUM traffic.	

Defect ID: DEFECT000608806	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** IPv6 Addressing
Symptom: Unexpected LP reload	
Condition: Shortly after reload	

Defect ID: DEFECT000609198	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: Unexpected LP reload.	
Condition: Flapping OSPF interfaces	

Defect ID: DEFECT000610574	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS Traffic Engineering
Symptom: Non-CSPF LSP may flap on a route update. One can notice this in the 'show mpls lsp extensive' command which logs the LSP event history. The LSP may remain DOWN until its state is cleaned up for that instance from the network. Traffic loss can be observed during this time if LSP is actively carrying traffic.	
Condition: Issue occurs when ALL the below conditions are true: - Adaptive LSP - Non-CSPF - Route update is seen on an LSP path	
Workaround: To avoid getting into this issue one can use CSPF LSPs instead if they already have Traffic Engineering configured under MPLS.	

Defect ID: DEFECT000611236	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.0.00	**Technology:** BGP/MPLS VPN
Symptom: L3VPN/VRF traffic is not forwarded.	
Condition: Change primary port of the LAG coupled with VRF config change on primary/secondary lag members.	
Workaround: If the LAG deploy/undeploy & add/del of member ports to LAG is as per Brocade Config Guide then the issue will not be seen.	

Defect ID: DEFECT000612470	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.8.00	**Technology:** MPLS Traffic Engineering
Symptom: LSP will not be established if LSP destination address is not the router id but any other address on the destination router.	
Condition: 1) Destination address of the LSP is not same as the router id of that destination router, but some other address on the router. 2) LSP nexthops are calculated if that destination router is the DR on that interface. Otherwise, LSP nexthops are not calculated.	

Defect ID: DEFECT000613850	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: The VRRP-E command "short-path-forwarding-delay <delayinseconds>" is not taking effect in IPv4 VRRP-E network ("router vrrp-extended").	
Condition: The issue will be noticed if "short-path-forwarding" command is used to configure the backup VRRP-E device as an alternate path in IPv4 VRRP-E network.	
Workaround: Disable "short-path-forwarding" and configure the "garp-ra-interval" to 2 seconds (using command - "garp-ra-interval <timeInSeconds>") on the VRRP-E instances in the IPv4 VRRP-E network.	

Defect ID: DEFECT000614649	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Multicast and Broadcast traffic may be dropped for up to 5sec during reloading or MM switchover on a MCT peer without linked CCEP	
Condition: Seen when performing a reload or management module switchover on an MCT peer with all edge ports including CCEP ports shutdown and only ICL and Spoke PW ports UP.	

Defect ID: DEFECT000614901	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** CLI - Command Line Interface
Symptom: Interfaces stay down on MLX 10Gx20 with 1G SFPs and do not come up even on disable/enable.	
Condition: The issue is seen when - chassis is loaded with default config, - MLX 10x20G card is inserted without the optics, and - 1G SFPs are then inserted fairly fast on the interfaces	

Defect ID: DEFECT000615076	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: With PIM-DM, “show ip pim mcache” shows OIFs continually added and deleted for a group. There is no traffic impact	
Condition: If PIM-DM is configured and multicast boundary for the group is applied only on incoming interface.	
Workaround: Apply multicast boundary for the group on both incoming and outgoing PIM-DM interfaces	
Recovery: Apply multicast boundary for the group on both incoming and outgoing PIM-DM interfaces	

Defect ID: DEFECT000617414	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.1.00	**Technology:** Software Installation & Upgrade
Symptom: During bootup, occasionally the user may encounter the following error related to flash. code_flash_block_erase: timeout, f91c0000: 80	
Condition: The error may occur during bootup without any user intervention. Bootup continues and system comes up as usual.	

Defect ID: DEFECT000617839	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: In MLX32/MLXe32 chassis, 1. card in any upper slot (17 to 32) of the chassis will display as" Invalid Module " in "show module" and the card will be in boot state 2. The card in the corresponding lower slot(1 to 16) may be rebooted continuously .	
Condition: 1. Issue occurs in MLX32/MLXe32 2. when any line card with incorrect PBIF FPGA version (of type 8x10G, 2x100G-SFP2, 2x100G-X, 4x40G, 20x10G, 4x10G-IPSEC) is inserted in upper slot(17 to 32) of the chassis, the line card in the corresponding lower slot will go for continuous reboot	
Recovery: Replace bad line card with good one	

Defect ID: DEFECT000619517	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.1.00	**Technology:** IGMP - Internet Group Management Protocol
Symptom: IGMP group version is not displayed correctly in "show ip igmp group" command	
Condition: When IGMP version is changed from 3 to 2 or from 2 to 3	

Defect ID: DEFECT000620069	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast VLAN Traffic Reduction
Symptom: Multicast traffic loss can be observed for VPLS.	
Condition: disabling and re-enabling of lag active primary port of VPLS end-point with Line card as BR-MLX-10Gx20.	

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: DEFECT000622734	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 06.0.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: LP-IPC task on LP module exception is happening after MM switch-over in MCT topology.	
Condition: 1) MCT cluster should be deployed. 2) VPLS instances has to be configured about 1000. 3)VPLS peers has to be configured. 4)MM switch-over has to be given in Active MCT.	

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

Defect ID: DEFECT000623624	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** ARP - Address Resolution Protocol
Symptom: Occasionally the first few packets across MCT cluster towards the host maybe dropped and the subsequent packets get forwarded.	
Condition: This occurs in MCT topology and affects routed packets when the ARP response from the host takes the path through ICL port. This is seen across all releases.	

Defect ID: DEFECT000624021	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** ACLs - Access Control Lists
Symptom: IPv6 rACL doesn't filter OSPF packets when the number of OSPF sessions on the same interface is more than 356.	
Condition: When user configures more than 356 OSPF neighbors on the same interface.	

Defect ID: DEFECT000624061	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** ICMP - Internet Control Message Protocol
Symptom: VE Interface MAC is not used as source MAC for packets routed by VPLS-VE interface.	
Condition: Save running configuration with VPLS VE and then reload. Or Copy Startup-Config with VPLS-VE configurations and then reload.	

Defect ID: DEFECT000624330	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.7.00	**Technology:** Traffic Queueing and Scheduling
Symptom: Egress traffic capped at 11% on port in BR-MLX-10Gx20 card even though the port is running at 10G speed.	
Condition: Issue noticed when the particular port on the BR-MLX-10Gx20 card in which the egress traffic is capped at 11% was booted up with a 1G optic and the 1G optic was replaced with a 10G optic after the line card became operationally "UP".	

Defect ID: DEFECT000624450	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Telemetry
Symptom: Errors may be incorrectly returned indicating that the command has failed	
Condition: When assigning noncontiguous ports to a GTP profile	

Defect ID: DEFECT000624554	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.8.00	**Technology:** Traffic Queueing and Scheduling
Symptom: VLL packets received from MPLS uplink are queued in Queue 0 on egress ports regardless of the EXP bit	
Condition: Seen on CER/CES platforms only.	

Defect ID: DEFECT000624579	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 06.1.00	**Technology:** MPLS Traffic Engineering
Symptom: Some LSPs go down on transit DUTs shortly after a reservable BW reduction on the protected path and data traffic loss is observed.	
Condition: The issue gets introduced on reducing the interface reservable bandwidth such that some of the LSPs get preempted and/or failover to their backups.	
Recovery: Re-signal affected LSPs from head-end router ("clear mpls lsp ...")	

Defect ID: DEFECT000624852	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.4.00	**Technology:** MRP - Metro Ring Protocol
Symptom: High LP CPU on MRP ring ports due to multicast traffic hitting through secondary path.	
Condition: If the MRP ring ports are trunk ports and multicast traffic is received through secondary path due to primary path down.	
Workaround: Configure the MRP ring ports as non-trunk interfaces	
Recovery: Clear the pim mcache on upstream PIM router in MRP ring which is wrongly forwarding traffic	

Defect ID: DEFECT000625240	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.0.00	**Technology:** IPv4 Multicast Routing
Symptom: Management Module may unexpectedly reload (and switches over to the standby Management Module if available). The following stack trace will be seen: - Possible Stack Trace (function call return address list) 211ea688: pim_process_candidate_rp_adv_msg(pc) 211ea500: pim_process_candidate_rp_adv_msg(lr) 211bb44c: receive_pimv2_packet 211ba630: receive_pimv2_packet_callback 20b8fe8c: itc_process_msgs_internal 20b90338: itc_process_msgs 21170a60: mcast_task 00005e18: sys_end_task	
Condition: Device should be configured as BSR Candidate. RP Candidate change notification is repeatedly triggered on the network and this device receives the updates.	

Defect ID: DEFECT000625655	
Technical Severity: High	**Probability:** High
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: OSPF adjacency proceeded to state FULL on one end and stuck at LOADING on other end of a link when network type mismatched. The adjacency need not be allowed to proceed to EXSTART in this case.	
Condition: Mismatched network type configured on both ends of a link - one end of the ospf link is set to type broadcast, and other end is set to point to point.	
Workaround: Ensure that both ends of link have same like type set (broadcast or p2p)	
Recovery: Change the configuration on one end of the link to match the link type of the other end.	

Defect ID: DEFECT000625732	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: Traffic is not sent to controller even though packets hit the OpenFlow rule and gets mirrored.	
Condition: Enable OpenFlow on the traffic ingress interface. Push an OpenFlow rule with action mirror port and send to controller. Witness the packet count for send to controller in output of "show openflow flow" is not getting incremented.	

Defect ID: DEFECT000625742	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: Management module may reload unexpectedly with the following stack trace: - Possible Stack Trace (function call return address list) 202e6cb0: parser(pc) 2035caa8: parse_input(lr) 20a80280: handle_new_line_from_telnet_client 20a80bdc: telnet_application_control 20a83fe8: telnet_receive_packet 20a82a14: telnet_socket_control 20a876b4: telnet_receive_data_ready 20a876f8: telnet_tcp_receive_data_ready_callback 20b92c64: itc_process_msgs_internal 20b9350c: itc_send_request_and_wait_internal 20b93ab0: itc_send_request_and_wait 20ab3cd4: lp_cli_show_value 20c51b10: cu_show_temperature_lp_all 2044d7c4: show_temperature_all_slot 2003456c: show_tech_support 203598b4: timer_callback_wrapper 20b92c64: itc_process_msgs_internal 20b9350c: itc_send_request_and_wait_internal 20b93ab0: itc_send_request_and_wait 20ab3cd4: lp_cli_show_value 20c51b10: cu_show_temperature_lp_all 20bfb724: cu_get_lp_temperature 2044d918: show_temperature_all_slot 2003456c: show_tech_support 2035	
Condition: In a telnet session, when pressing "Enter" key continuously during the "show tech-support" command execution.	

Defect ID: DEFECT000626266	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: There will be higher CPU utilization after receiving around or more than 500 OSPFv2 Type-5 LSAs.	
Condition: Running OSPFv2 protocol with VRF-lite.	

Defect ID: DEFECT000626429	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** Multi-VRF
Symptom: IPv6 traffic received on non-default VRF doesn't get rate-limited as per the configured rate-limiting on interface.	
Condition: IPv6 ACL based rate-limiting configured on interface for non-default VRF	

Defect ID: DEFECT000627306	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: Remote port connected to a loopback configured port goes down	
Condition: Reloading line card that has a loopback configured port	
Recovery: Disable and enable the loopback configured port	

Defect ID: DEFECT000627353	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.0.00	**Technology:** OpenFlow
Symptom: When 512 OpenFlow rules or more are configured having the same output port as logical MPLS port (LSP), the LP software is getting reloaded unexpectedly, if the LSP goes down and comes up.	
Condition: Enable OpenFlow on LSP. Configure 512 flows or more with output as OpenFlow logical port (LSP) Make the LSP go down by disabling the mpls-interface.	

Defect ID: DEFECT000627906	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 06.1.00	**Technology:** IPv6 Multicast VLAN Traffic Reduction
Symptom: MLD snooping switch connected directly to receivers may see high CPU utilization on ingress line-card due to IPv6 multicast data traffic.	
Condition: High CPU utilization on ingress line-card happens due to IPv6 multicast snooping entries not created in MP for some reason.	

Defect ID: DEFECT000628596	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: On CES/CER, MCT node forwards multicast traffic out of the same MCT lag from which the MCT peer receives the traffic.	
Condition: Add a member-VLAN to the MCT cluster	

Defect ID: DEFECT000629528	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 06.1.00	**Technology:** OpenFlow
Symptom: Traffic loss when traffic going on OpenFlow Logical port group which contain LSP tunnels, configured on both physical port and lag	
Condition: Egress port is OpenFlow Logical Port Group contains LSP tunnels going on Physical ports and LAG.	
Workaround: Make LSP tunnels either going to Physical ports or LAG ports.	

Defect ID: DEFECT000626014	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Multicast and Broadcast data traffic may be dropped for up to 4-5sec when CCP goes down by reloading or MM switchover on a MCT peer.	
Condition: In a MCT network setup, CCP down event due to - MCT peer reload or - MCT peer management module switchover will cause this condition	