20 June 2017

NI OS 6.0.00a for Brocade MLXe and NetIron

Release Notes v4.0

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial release	08/11/16
2.0	Updated limitations section for 802.1BR and VN-tag header processing.	08/16/16
3.0	Updated Closed with code changes R06.0.0.	08/26/16
4.0	Moved Defect000591202 from the Known Issues list to Closed with code changes R06.0.00a list.	06/20/17

Preface

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • **My Cases through MyBrocade** • **Software downloads and licensing tools** • **Knowledge Base**	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and • Asia Pacific: +800-AT FIBREE • (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Related documentation

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

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

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

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

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

Overview

NetIron OS Release 6.0.00 introduces new functionalities and enhances the capabilities of Brocade MLX Series, CER 2000 Series and CES 2000 Series. Brocade continues to innovate in key technologies and Release 6.0.00 brings new features in the following areas:

- SDN,
- Data privacy with IPsec,
- IP/MPLS services,
- Network Packet Broker functionality for 4G/LTE mobile networks and
- New Optics for 40G connectivity options.

Path Computation Element Protocol and OpenFlow to MPLS LSP as logical port allow service providers to migrate to an SDN operation model while maintaining interoperability with existing MPLS networks.

Layer 2 over IPsec enables secure connections for data center interconnect and enterprises can now meet security compliances in the public clouds and virtual private clouds.

In addition, manageability and troubleshooting functions are further enhanced for efficient network operation. With these features, Brocade MLX Series Router continues as the leading platform for converged data center and service provider network services.

Brocade MLXe Network Packet Broker

Beginning with NetIron 6.0.00a two FPGA bundles will be available for download.

- Installing the Network Packet Broker (NPB) FPGA bundle will place the Brocade MLXe device chassis into Packet Broker mode.
- Installing the MAIN (default) FPGA bundle will place the Brocade MLXe device chassis into the default mode.

The global setting across the chassis can be either Network Packet Broker (NPB) mode or MAIN (default).

- The Main (default) global setting requires the MAIN FPGA manifest to be installed.
- The NPB global setting requires the NPB FPGA manifest to be installed.

Behavior changes

Behavior changes in release

- 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 R06.0.00a.

Software Features

New software features introduced in R06.0.00a

Network Packet Broker Enhancements:

Starting in the R06.0.00a release, some Network Packet Broker (NPB) features are enabled only on the NPB FPGA. If you are using any of the following features in NPB deployments on the following line cards, please ensure that you are using the correct NetIron 6.0.00a NPB FPGA files. All the other NPB features are enabled on all line cards and on both the Main and NPB FPGAs.

MLXe Module	NPB FPGA	Main FPGA
BR-MLX-10Gx20	• Packet Timestamping • NVGRE stripping • Source port labeling	Following NPB features Not Present: • Packet Timestamping • NVGRE stripping • Source port labeling
BR-MLX-40Gx4	Not Applicable	• Packet Timestamping • NVGRE stripping • Source port labeling
BR-MLX-100Gx2	• Packet Timestamping • NVGRE stripping • Source port labeling	Following NPB features Not Present: • Packet Timestamping • NVGRE stripping • Source port labeling

The following features are the new NPB features:

- **802.1BR and VN-Tag stripping:** This feature strips 802.1br header (ether-type=0x893f) and VN-tag header (ether-type=0x8926) from ingress traffic before sending it for further processing/forwarding. This is useful in cases where the analytics tools do not understand these headers.
- **Packet Timestamping:** This feature allows inserting an 8-byte timestamp into ingress packets. The timestamp can be NTP time or local clock time.
- **SCTP traffic filtering:** This feature enables the user to filter SCTP traffic based on source and destination TCP/UDP ports.
- **Source port labeling**: Users can enable this feature to insert a 4-byte label to identify the ingress port. This source port label will hold the SNMP IfIndex value from IFMIB for the interface. Source port is used for downstream filtering.
- **NVGRE stripping:** The NVGRE header-stripping feature enables the user to strip the outer Ethernet, Outer IPv4, and the NVGRE header from incoming IPv4 NVGRE packets. This is useful in cases where the analytics tools do not understand these headers, or if the tool is only interested in the tunneled information.
- **Packet Length filtering:** This feature allows users to filter ingress IPv4 and IPv6 traffic based on IP Payload Length of packets. For IPv4, payload length excludes IP header length. For IPv6, there is already a Payload Length field present in the header.

The following features are the other new features:

SNMP/MIB Changes:

- **PCEP MIB:** This feature will provide MIB support to track the status and statistics of PCEP related information. The following tables and notifications are supported: PcePcepEntityTable, PcePcepPeerTable, PcePcepSessTable, pcePcepSessUp, pcePcepSessDown, pcePcepSessPeerOverload, pcePcepSessPeerOverloadClear"
- **Auto-bandwidth MIB:** This MIB (mplsLspAutoBwTable) will help monitor status and statistics of MPLS RSVP auto-bandwidth related information via SNMP
- **SNMP support for CAM utilization (PRODRFE103262):** CAM usage can be monitored via SNMP MIBs. This feature aligns MIBs to the current CAM partition/sub-partition structure.

OpenFlow Enhancements:

- **OpenFlow: ARP to normal plus controller:** With this feature along with regular processing of ARP (consumed by CPU or flooded in bridge/vlan domain), punting of ARP packets to the SDN controller is also supported when the SDN controller programs such a flow rule. ARP packets can be tagged or untagged coming in on configured unprotected VLAN.

- **OpenFlow support for MPLS as switched:** When ingress MPLS traffic with no interface MAC is received on an openflowL2/L23 interface, it will be switched and will not hit the MPLS OpenFlow rule.
- **Primary Port LAG:** This feature changes primary port in LAG with no traffic disruption. Prior to this release, primary port change was manual and caused traffic disruption. Starting with NetIron 6.0.00a, the change will be seamless with no traffic disruption.
- **AAA local authentication fallback (PRODRFE103246):** This feature allows the administrator to fallback to the local authentication method in case a server in a previous authentication method returned access-reject. Prior to this release this was done only in case there was a timeout from servers of earlier methods. In case of authentication success from the server, that response is considered final for that method and the entire authentication.
- **DH group 14 for SSH in non-FIPS mode (PRODRFE103457):** In earlier releases, the Diffie Hellman Group 14 is supported for FIPS and CC mode only. With this feature enhancement DH Group 14 is supported in regular mode (for example, when FIPS is not enabled) as well.
- **CE2.0 Change in MLXe**: Rate-limiting function was enhanced to meet CE2.0 guidelines to enable certification.
- **Ingress ACL permit logging:** This feature when enabled will log packets matching the permit rule of an access-list for IPv4 and IPv6. It is supported for ingress filtering only, and can be enabled for User ACL and rACL bindings. It is not supported for L2ACLs. Logging can be done selectively as well with optional CLI to limit CPU utilization.
- **PKI offline enrollment:**

  This feature introduces the following enhancements to PKI certificate management:

  - **Offline certificate Enrollment:** Device will generate CSR and prints it to console and copies a file to flash in base64 format. User can manually take the CSR to CA server and can obtain the certificate. Then User can load the certificate into a device. Useful in case the CA server needs to be offline.
  - **Offline loading of certificates and CRLs:** User can paste the PEM format certificate or CRL onto device console now.
  - **Certificate chain validation using CRLs:** Previously when using CRL, only the revocation status of peer's client certificate is validated not the whole chain. With this enhancement, we validate the revocation status of entire peer certificate chain including CA certificates.

Optics Support:

Support for QSFP 28 Optics.

Software features introduced in R06.0.00

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

IPsec enhancements:

- L2 over IPsec – The feature provides secure point to point layer 2 extension over WAN. The layer 2 traffic is encrypted by IPsec tunnels using the most advanced Suite-B security protocols.
- ICX IPsec interoperability - ICX and MLXe have been tested to interoperate in the same IPsec tunnels for secure VPN connection for enterprise.
- vRouter IPsec interoperability - vRouter and MLXe have been tested to interoperate in the same IPsec tunnels for secure VPN connection between enterprise data center and public cloud for hybrid cloud use case.
- Track IPsec tunnels for VRRP failover - If the IPsec tunnel goes down, the VRRP / VRRPe priority will decrement and trigger the failover the VRRP / VRRPe peers.
- Option to display IKEv2 debug for a particular IPsec tunnel - The debug option displays IKEv2 debug logs for a specific IPSec tunnel as configured by the user. The debug logs are as per the currently supported debug logs such as trace, event, error, packet et cetera.

Software-defined Network (SDN):

- Path Computing Element Communication Protocol (PCEP) - Path Computing Element (PCE) is SDN based solution for MPLS traffic engineering. MLXe will act as the PCE client (PCC) that will request RSVP LSP path calculation from the PCE server. PCE server will inquire its own traffic engineering database and respond with the explicit path object to the PCC. Stateless PCE based on RFC 5440 will be supported in NI 6.0.
- OpenFlow to MPLS LSP as logical port - MPLS LSP tunnels are supported in OpenFlow as logical ports.

Network Packet Broker enhancements:

- Increase traffic streams to 6K - The number of traffic streams / transparent VLANs is increased to 6K to support high scale network packet broker and telemetry functions.
- Increase L2 and L3 ACL to 4K - The number of Layer 2 and Layer 3 ACLs is increased to 4K to support high scale packet filtering.
- SNMP monitoring support L2 ACL - SNMP monitoring is enabled for L2 ACL through MIB.
- High/low watermark thresholds for traffic statistics - The high and low watermarks for the past 1 hour and past 24 hours of each physical interface will be tracked for interface statistics.
- IPv6 ACL .1p match - It allows user to filter IPv6 traffic on the basis of .1p priority.

BGP diverse path:

- BGP Add-Path - This enables router to advertise multiple paths for the same prefix for multi-pathing and faster convergence.

- BGP Best External - The router can advertise the best external BGP path to the BGP neighbors even when it receives a better internal BGP route. This enable multiple exit paths to other AS.

GRE enhancements:

- GRE tunnel bypassing ACL - An option is added to allow traffic coming in from the GRE tunnel to bypass the ACL configured on the interface.
- GRE tunnel to hand off to MPLS - This allows GRE tunnel to hand off to MPLS LSP
- IPv6 over IPv4 GRE - IPv6 traffic can be carried across IPv4 GRE tunnels.

IPv6 enhancements:

- IPv6 for VE over VPLS - IPv6 addresses and IPv6 routing will be supported on VE over VPLS interfaces.
- IPv6 ACL deny logging - The IPv6 ACL deny logging feature records traffic flows that are denied by IPv6 inbound ACLs. When a packet is denied by an ACL, a syslog entry is generated.
- IPv6 ACL per SNMP server group - IPv6 ACLs can be applied to individual SNMP server group to limit access at a per group level.

New Optics:

- 40G Bi-Di QSFP – 40G Bi-Di QSFP+ optics is now supported on the MLXe 4-port 40G line card.

Other features:

- BFD Support across MCT - BFD is supported on routers in MCT to provide connectivity check for faster route convergence.
- Load balance VLL to a specific group of LSPs - Traffic from VLL can be load balanced up to 8 LSPs.
- Radius over TCP / TLS - Radius connection will be sent over TCP (RFC 6613) and also over TLS (RFC 6614) to provide encrypted RADIUS.
- Increase Netconf RPC response limit to 512K - The RPC response limit to a NETCONF client has been increased to 512 Kbytes. It is 32 Kbytes in previous releases.
- LDP shortcut - Router generated packets such as routing protocols and OAM packets (pings and traceroutes) can be sent over MPLS LDP tunnels instead of regular IP routing.
- Multicast snooping per flag aging - The multicast snooping database will age out per flag.
- IPC stuck auto detection on LP and MP - This feature generates syslog's to indicate when IPC Tx queue is stuck when the queue is non-empty.
- Show tech additions - The following show tech sub-commands have been added.
  Show cpu histogram hold no clear
  Show cpu histogram wait noclear
  Show tm log
  Show tm histogram

Show tm non-empty-queue
Itc show statistics
Itc show error list
Statistics for IPC Retransmits from MP

- Show command for disabled CCEP port with MCT Spoke PW status - This show command is to display the MCT spoke PW state for both L2 and L2VPN client ports.
- MCT CCEP port up delay - A configurable delay is added to LACP-BLOCKED state after CCEP port is enabled to prevent duplicate L2 BUM packets.
- High CPU auto detection on MP - The MP CPU is monitored regularly. If the CPU crosses a threshold, log file will be created for troubleshooting.
- LSP down syslog reason string - This feature adds a reason string to LSP down syslog to explain what causes the LSP to go down
- IPC statistics show TX drops – New fields are added to show the drops in reliable and unreliable transmit under the ipc show statistics command

CLI commands

The following commands are new in this release.

New CLI commands R06.0.00a

- [no] fpga_mode_npb
- [no] lag port-primary-dynamic
- [no] port-primary-dynamic
- [no] lacp system-priority *number*
- [no] strip-802-1br all
- [no] strip-vn-tag slot *slot-num*
- [no] strip-802-1br slot *slot-num* device *device-id*
- [no] strip-vn-tag all
- [no] strip-vn-tag slot *slot-num*
- [no] strip-vn-tag slot *slot-num* device *device-id*
- show packet-encap-processing
- show packet-encap-processing strip-802-1BR
- show packet-encap-processing strip-vn-tag
- show packet-encap-processing [slot slot-num]
- show packet-encap-processing interface Ethernet
- show running-config – (for config-pkt-encap-proc mode)
- ip match-payload-len
- ipv6 match-payload-len
- show ip match-payload-len
- show ip match-payload-len [interface ethernet slot | port]
- show ipv6 match-payload-len
- show ipv6 match-payload-len [interface ethernet slot | port]
- [no] config-pkt-encap-proc

Modified commands in Brocade Network Packet Broker R06.0.00a

- The show version and show flash command output will include information about whether the XPP FPGA on an LP is NPB. If there is no reference to NPB in the command output, it is the MAIN FPGA.

CLI commands introduced in R06.0.00

- additional-paths
- additional-paths select
- advertise-best-external
- clear np qos statistics
- client-interfaces sync_ccep_early
- dead-timer
- disable-acl-for-6to4
- disable-acl-for-gre
- enable pce
- enable-qos-statistics
- match additional-paths advertise-set
- message-bundle-support
- max-unknown-messages
- max-unknown-requests
- min-keepalive
- negotiation-deny
- neighbor additional-paths
- neighbor additional-paths advertise
- new additional-paths disable
- pce compute
- preference
- request-timer
- router pcep
- set next-hop-tvf-domain
- show acl-policy
- show tvf-domain
- suppress-ipv6-priority-mapping
- sysmon mp-high-cpu enable
- sysmon mp-high-cpu cpu-threshold
- sysmon mp-high-cpu task-threshold
- sysmon ipc rel-q-mon enable
- trv-domain

- vll-peer (load-balance)

Modified commands in R06.0.00

The following commands have been modified in this release.

- ipv6 access-list
- interface ve
- set next-hop-tvf-domain
- show cluster
- show ipsec profile
- show ip multicast
- show ip multicast vpls
- show ip route
- show ipv6 bgp neighbors
- show ipv6 bgp routes
- show np qos statistics
- show mpls vll
- show run
- sysmon np memory-errors action
- track-port
- vll-peer
- vll-peer (load balance)

Deprecated commands

There are no deprecated commands in this release.

MIBs and messages

MIBs

New MIB Objects

The following MIB objects are new in this release:

- fdryL2AclIfBindAclName – New OID
- fdryL2NamedAclTable - New table
    - fdryL2NamedAclIndex
    - fdryL2NamedAclClauseIndex
    - fdryL2NamedAclName
    - fdryL2NamedAclAction
    - fdryL2NamedAclSourceMac
    - fdryL2NamedAclSourceMacMask
    - fdryL2NamedAclDestinationMac
    - fdryL2NamedAclDestinationMacMask
    - fdryL2NamedAclVlanId
    - fdryL2NamedAclEthernetType
    - fdryL2NamedAclDot1pPriority
    - fdryL2NamedAclDot1pPriorityForce
    - fdryL2NamedAclDot1pPriorityMapping
    - fdryL2NamedAclMirrorPackets
    - fdryL2NamedAclLogEnable
    - fdryL2NamedAclRowStatus
- bgp4V2NlriRxPathIdentifier – New OID
- bgp4V2NlriTxPathIdentifier – New OID
- IfXWatermarkTable – New Table
    - ifWatermarkCurrentHourWindowStartTime
    - ifWatermarkCurrentHourHighRxUtilTime
    - ifWatermarkCurrentHourHighInPktRate
    - ifWatermarkCurrentHourHighInBitRate
    - ifWatermarkCurrentHourLowRxInUtilTime
    - ifWatermarkCurrentHourLowInPktRate
    - ifWatermarkCurrentHourLowInBitRate
    - ifWatermarkCurrentHourHighTxUtilTime
    - ifWatermarkCurrentHourHighOutPktRate
    - ifWatermarkCurrentHourHighOutBitRate
    - ifWatermarkCurrentHourLowTxOutUtilTime
    - ifWatermarkCurrentHourLowOutPktRate
    - ifWatermarkCurrentHourLowOutBitRate
    - ifWatermarkLastHourHighRxUtilTime
    - ifWatermarkLastHourHighInPktRate
    - ifWatermarkLastHourHighInBitRate
    - ifWatermarkLastHourLowRxUtilTime
    - ifWatermarkLastHourLowInPktRate

- ifWatermarkLastHourLowInBitRate
- ifWatermarkLastHourHighTxUtilTime
- ifWatermarkLastHourHighOutPktRate
- ifWatermarkLastHourHighOutBitRate
- ifWatermarkLastHourLowTxUtilTime
- ifWatermarkLastHourLowOutPktRate
- ifWatermarkLastHourLowOutBitRate
- ifWatermarkCurrentDayWindowStartTime
- ifWatermarkCurrentDayHighRxUtilTime
- ifWatermarkCurrentDayHighInPktRate
- ifWatermarkCurrentDayHighInBitRate
- ifWatermarkCurrentDayLowRxInUtilTime
- ifWatermarkCurrentDayLowInPktRate
- ifWatermarkCurrentDayLowInBitRate
- ifWatermarkCurrentDayHighTxUtilTime
- ifWatermarkCurrentDayHighOutPktRate
- ifWatermarkCurrentDayHighOutBitRate
- ifWatermarkCurrentDayLowTxOutUtilTime
- ifWatermarkCurrentDayLowOutPktRate
- ifWatermarkCurrentDayLowOutBitRate
- ifWatermarkLastDayHighRxUtilTime
- ifWatermarkLastDayHighInPktRate
- ifWatermarkLastDayHighInBitRate
- ifWatermarkLastDayLowRxUtilTime
- ifWatermarkLastDayLowInPktRate
- ifWatermarkLastDayLowInBitRate
- ifWatermarkLastDayHighTxUtilTime
- ifWatermarkLastDayHighOutPktRate
- ifWatermarkLastDayHighOutBitRate
- ifWatermarkLastDayLowTxUtilTime
- ifWatermarkLastDayLowOutPktRate
- ifWatermarkLastDayLowOutBitRate

Deprecated MIBs

There are no deprecated MIBs in this release.

RFCs and standards

The following RFCs and standards are newly supported in this release:

- draft-ietf-idr-add-paths-10
- draft-ietf-idr-best-external-05
- RFC 4655 – A Path Computation Element (PCE) Based Architecture.
- RFC 5440 – Path Computation Element (PCE) Protocol (PCEP). Fully supported except SVEC and Load-balance objects
- RFC 5521 – Extensions to the Path Computation Element Protocol (PCEP) for Route Exclusions. This is partially supported; SRLG ID and Unnumbered interfaces are not supported. Explicit Exclusion Route sub-object (EXRS) is not supported.

Hardware support

Supported devices for R06.0.00a

The following devices are supported in this release:

- Brocade NetIron XMR 4000
- Brocade NetIron XMR 8000
- Brocade NetIron XMR 16000
- Brocade NetIron XMR 32000
- Brocade MLX-4
- Brocade MLX-8
- Brocade MLX-16
- Brocade MLX-32
- Brocade MLXe-4
- Brocade MLXe-8
- Brocade MLXe-16
- Brocade MLXe-32
- Brocade NetIron CES 2024C-4X
- Brocade NetIron CES 2024F-4X
- Brocade NetIron CER-RT 2024C-4X
- Brocade NetIron CER-RT 2024F-4X
- Brocade NetIron CES 2024C
- Brocade NetIron CES 2024F
- Brocade NetIron CES 2048C
- Brocade NetIron CES 2048CX
- Brocade NetIron CES 2048F
- Brocade NetIron CES 2048FX
- Brocade NetIron CER 2024C
- Brocade NetIron CER-RT 2024C
- Brocade NetIron CER 2024F
- Brocade NetIron CER-RT 2024F
- Brocade NetIron CER 2048C
- Brocade NetIron CER-RT 2048C
- Brocade NetIron CER 2048CX
- Brocade NetIron CER-RT 2048CX
- Brocade NetIron CER 2048F
- Brocade NetIron CER-RT 2048F
- Brocade NetIron CER 2048FX
- Brocade NetIron CER-RT 2048FX

Supported devices for Brocade Network Packet Broker R06.0.00a

- Brocade NetIron XMR 4000
- Brocade NetIron XMR 8000
- Brocade NetIron XMR 16000
- Brocade NetIron XMR 32000
- Brocade MLX-4
- Brocade MLX-8
- Brocade MLX-16
- Brocade MLX-32
- Brocade MLXe-4
- Brocade MLXe-8
- Brocade MLXe-16
- Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade MLX 2-port 100 GbE (M) CFP2 module. Supports 512,000 IPv4 routes in FIB.	Yes	Yes	3
BR-MLX-100GX2-CFP2-X2	Brocade 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-100GX1-X	Brocade 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	Brocade 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-10GX8-X	Brocade MLX Series 8-port 10 GbE (X) module with IPv4/IPv6/MPLS hardware support—requires SFP optics. Supports up to 1 million IPv4 routes in FIB. Requires high-speed switch fabric modules.	Yes	Yes	2
BR-MLX-1GCX24-X	Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade 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	Brocade 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-1GX48-T-A	Brocade MLX Series 48-port 10/100/1000BASE-T, MRJ21 module with IPv4/IPv6/MPLS hardware support.	Yes	No	1.1
NI-MLX-10GX8-D	Brocade 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	Brocade 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	Brocade 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 Brocade, refer to the latest version of the Brocade Optics Family Data Sheet available online at www.brocade.com.

The NetIron 6.0.00a release includes support for the following:

Part number	Description
CFP2-TO-QSFP28-MOD	CFP2 to QSFP28 conversion module

Software upgrade and downgrade

Image file names

Download the following images from www.brocade.com. In some cases boot and manifest images do not need to be upgraded.

Brocade 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 R6.0.00a MLX Series/XMR software upgrade

Manifest File for XMR/MLX Release 06.0.00

-NETIRON_IRONWARE_VER XMR-MLXV6.0.00a
#==========
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin
-DIRECTORY /Boot/ManagementModule
xmprm05900.bin
Application Images
-DIRECTORY /Combined/FPGA
lpfpga06000a.bin
-DIRECTORY /Combined/Application
xm06000a.bin
-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin
-DIRECTORY /Monitor/ManagementModule
xmb06000.bin
-DIRECTORY /Application/ManagementModule
xmr06000a.bin
-DIRECTORY /Application/InterfaceModule
xmlp06000a.bin
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06000a.bin 2.05
pbif8x10_06000a.bin 2.24
pbifmrj_06000a.bin 4.04
pbifsp2_06000a.bin 4.02
statsmrj_06000a.bin 0.09
xgmacsp2_06000a.bin 0.17
xpp2x100_06000a.bin 1.05
xpp4x40_06000a.bin 6.00
xpp4x10g3_06000a.bin 5.00
xpp8x10_06000a.bin 1.04
xppmrj_06000a.bin 1.01

xppsp2_06000a.bin 1.01
xppxsp2_06000a.bin 1.01
pbif-ber-g3_06000a.bin 2.05
xpp20x10g3_06000a.bin 6.04
xpp2x100g3_06000a.bin 6.04

-DIRECTORY /FPGA/ManagementModule
mbridge32_06000a.xsvf 36
mbridge_06000a.xsvf 37
sbridge_06000a.mcs 6
hsbridge_06000a.mcs 17
-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06000.sig
xmb06000.sig
xmr06000a.sig
xmlp06000a.sig
lpfpga06000a.sig
hsbridge_06000a.sig
mbridge_06000a.sig
mbridge32_06000a.sig
sbridge_06000a.sig
pbif4x40_06000a.sig
pbif8x10_06000a.sig
pbifmrj_06000a.sig
pbifsp2_06000a.sig
pbif-ber-g3_06000a.sig
statsmrj_06000a.sig
xgmacsp2_06000a.sig
xpp2x100_06000a.sig
xpp20x10g3_06000a.sig
xpp2x100g3_06000a.sig
xpp4x40_06000a.sig
xpp4x10g3_06000a.sig
xpp8x10_06000a.sig
xppmrj_06000a.sig
xppsp2_06000a.sig
xppxsp2_06000a.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
xmr06000a.sha256
xmlp06000a.sha256
lpfpga06000a.sha256

hsbridge_06000a.sha256
mbridge_06000a.sha256
mbridge32_06000a.sha256
sbridge_06000a.sha256
pbif4x40_06000a.sha256
pbif8x10_06000a.sha256
pbifmrj_06000a.sha256
pbifsp2_06000a.sha256
pbif-ber-g3_06000a.sha256
statsmrj_06000a.sha256
xgmacsp2_06000a.sha256
xpp2x100_06000a.sha256
xpp20x10g3_06000a.sha256
xpp2x100g3_06000a.sha256
xpp4x40_06000a.sha256
xpp4x10g3_06000a.sha256
xpp8x10_06000a.sha256
xppmrj_06000a.sha256
xppsp2_06000a.sha256
xppxsp2_06000a.sha256

FPGA file names and supported modules

File Name	Supported Modules
pbif4x40	4x40G modules
pbif8x10	8x10G modules
pbifmrj	24x1G and 48x1G modules
pbifsp2	2x10G, 4x10G, 4x10G-x and 20x1G modules
statsmrj	24x1G and 48x1G modules
xgmacsp2	2x10G, 4x10G-x and 4x10G modules
xpp2x100	2x100G modules (double-wide CFP-based module)
xpp4x40	4x40G modules
xpp8x10	8x10G modules
File Name	**Supported Modules**
xppmrj	24x1G and 48x1G modules
xppsp2	2x10G, 4x10G, and 20x1G modules
xpp4x10g3	4x10G and 4x1G (M) IPSEC modules
xppxsp2	4x10G-x
pbif-ber-g3	20x10G and 2x100G modules (-M and –X2)
xpp20x10g3	20x10G modules
xpp2x100g3	2x100G modules (half-slot CFP2-based module)

mbridge32	MBRIDGE32
mbridge	MBRIDGE
sbridge	Switch fabric modules
hsbridge	High speed switch fabric modules

Brocade 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-CERV6.0.00a
#==========
-DIRECTORY /Boot
ceb06000.bin
-DIRECTORY /Application
ce06000a.bin
-DIRECTORY /FPGA
pbifmetro_06000a.bin
-END_OF_IMAGES

-DIRECTORY /Signatures
ceb06000.sig
ce06000a.sig
pbifmetro_06000a.sig
ceb06000.sha256
ce06000a.sha256
pbifmetro_06000a.sha256

Manifest for Brocade 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 R6.0a software upgrade

-NETIRON_IRONWARE_VER XMR-MLXV6.0.00a
#==========
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin
-DIRECTORY /Boot/ManagementModule
xmprm05900.bin

Application Images
-DIRECTORY /Combined/FPGA
lpfpga_npb_06000a.bin
-DIRECTORY /Combined/Application
xm06000a.bin
-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin
-DIRECTORY /Monitor/ManagementModule
xmb06000.bin
-DIRECTORY /Application/ManagementModule
xmr06000a.bin
-DIRECTORY /Application/InterfaceModule
xmlp06000a.bin
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06000a.bin 2.05
pbif8x10_06000a.bin 2.24
pbifmrj_06000a.bin 4.04
pbifsp2_06000a.bin 4.02
statsmrj_06000a.bin 0.09
xgmacsp2_06000a.bin 0.17
xpp2x100_06000a.bin 1.05
xpp4x40_06000a.bin 6.00
xpp4x10g3_06000a.bin 5.00
xpp8x10_06000a.bin 1.04
xppmrj_06000a.bin 1.01
xppsp2_06000a.bin 1.01
xppxsp2_06000a.bin 1.01
pbif-ber-g3_06000a.bin 2.05
xpp20x10g3_npb_06000a.bin
xpp2x100g3_npb_06000a.bin
-DIRECTORY /FPGA/ManagementModule
mbridge32_06000a.xsvf 36
mbridge_06000a.xsvf 37
sbridge_06000a.mcs 6
hsbridge_06000a.mcs 17
-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06000.sig
xmb06000.sig
xmr06000a.sig
xmlp06000a.sig
lpfpga_npb_06000a.sig
hsbridge_06000a.sig
mbridge_06000a.sig
mbridge32_06000a.sig

sbridge_06000a.sig
pbif4x40_06000a.sig
pbif8x10_06000a.sig
pbifmrj_06000a.sig
pbifsp2_06000a.sig
pbif-ber-g3_06000a.sig
statsmrj_06000a.sig
xgmacsp2_06000a.sig
xpp2x100_06000a.sig
xpp20x10g3_npb_06000a.sig
xpp2x100g3_npb_06000a.sig
xpp4x40_06000a.sig
xpp4x10g3_06000a.sig
xpp8x10_06000a.sig
xppmrj_06000a.sig
xppsp2_06000a.sig
xppxsp2_06000a.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
xmr06000a.sha256
xmlp06000a.sha256
lpfpga_npb_06000a.sha256
hsbridge_06000a.sha256
mbridge_06000a.sha256
mbridge32_06000a.sha256
sbridge_06000a.sha256
pbif4x40_06000a.sha256
pbif8x10_06000a.sha256
pbifmrj_06000a.sha256
pbifsp2_06000a.sha256
pbif-ber-g3_06000a.sha256
statsmrj_06000a.sha256
xgmacsp2_06000a.sha256
xpp2x100_06000a.sha256
xpp20x10g3_npb_06000a.sha256
xpp2x100g3_npb_06000a.sha256
xpp4x40_06000a.sha256
xpp4x10g3_06000a.sha256
xpp8x10_06000a.sha256
xppmrj_06000a.sha256
xppsp2_06000a.sha256
xppxsp2_06000a.sha256

Migration path

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

Upgrade and downgrade considerations

To upgrade to 6.0.00a, a two-step approach may be required. The two-step upgrade process is not required for CER or CES. The two-step process is applicable to MLXe and XMR only.

Scenario 1

Customers running releases 5.9.00a, 5.6.00ga, 5.6.00h, 5.8.00d, 5.7.00e or subsequent releases can directly upgrade to 6.0.00a using MLX06000a_Manifest.txt.

NOTE: If the System is not running one of the releases listed above, follow scenario 2 or scenario 3 mentioned below.

Scenario 2

To upgrade from 5.6.00c or any later release (other than the images mentioned in Scenario 1), a two-step approach is required.

1. Upgrade to 5.9.00b and reload the device.
2. Upgrade to 6.0.00a using MLX06000a_Manifest and reload the device.

Scenario 3

To upgrade to 6.0.00a from releases prior to R05.6.00c, use the following procedure.

1. Upgrade to 5.9.00b and reload the device.
2. Upgrade again to 5.9.00b 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 6.0.00a with MLX06000a_Manifest.txt and reload the device.

Scenario 4

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

- Packet Timestamping
- Source port labeling
- NVGRE stripping

1. Upgrade to 6.0.00a using any of above scenarios based on the image from which the upgrade is being performed.
2. Reload the device again and verify that the system is up with NI 6.0.00a.
3. Configure the **fpga-mode-npb** command and save the configuration.
4. Upgrade to the 6.0.00a NPB image using MLX_npb_06000a_Manifest.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

```
MLX-GVR#show version
System Mode: XMR

...
...
...
FPGA versions:
Valid PBIF Version = 2.05, Build Time = 5/20/2015 22:20:00

Valid XPP Version = 6.14 (NPB), Build Time = 5/18/2016 17:39:00

MACXPP100G 0
MACXPP100G 1
1199 MHz MPC P2010 (version 8021/1051) 599 MHz bus
512 KB Boot Flash (MX29LV040C), 66846720 Bytes (~64 MB) Code Flash (MT28F256J3)
3072 MB DRAM, 8 KB SRAM
...
...


Boot     : Version 5.9.0T175 Copyright (c) 1996-2015 Brocade Communications Systems,
Inc.
Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900
 (449576 bytes) from boot flash
Monitor  : Version 6.0.0T175 Copyright (c) 1996-2015 Brocade Communications Systems,
Inc.
Compiled on Jun  7 2016 at 16:09:50 labeled as xmlb06000
```

```
 (571513 bytes) from code flash
IronWare : Version 6.0.0aT177 Copyright (c) 1996-2015 Brocade Communications Systems,
Inc.
Compiled on Jul 25 2016 at 11:27:22 labeled as xmlp06000a
 (9529041 bytes) from Primary
FPGA versions:
Valid PBIF Version = 2.05, Build Time = 5/20/2015 22:20:00

Valid XPP Version = 6.14 (NPB), Build Time = 5/2/2016 12:00:00

...
...
...

All show version done
MLX-GVR#
```

Output example for the show flash command

```
MLX-GVR#show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
...
...
...

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 1
Code Flash: Type MT28F256J3, Size 66846720 Bytes (~64 MB)
  o IronWare Image (Primary)
    Version 6.0.0aT177, Size 9529041 bytes, Check Sum a2c5
    Compiled on Jul 25 2016 at 11:27:22 labeled as xmlp06000a
  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 = 2.05, Build Time = 5/20/2015 22:20:00

 XPP Version = 6.14 (NPB), Build Time = 5/18/2016 17:39:00

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 2
Code Flash: Type MT28F256J3, Size 66846720 Bytes (~64 MB)
  o IronWare Image (Primary)
    Version 6.0.0aT177, Size 9529041 bytes, Check Sum a2c5
    Compiled on Jul 25 2016 at 11:27:22 labeled as xmlp06000a
  o IronWare Image (Secondary)
    Version 5.7.0T177, Size 7794476 bytes, Check Sum 5e0c
    Compiled on Jun 26 2014 at 12:16:28 labeled as xmlp05700
  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 = 2.05, Build Time = 5/20/2015 22:20:00

 XPP Version = 6.14 (NPB), Build Time = 5/2/2016 12:00:00

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
...
...
...

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 16
Code Flash: Type MT28F256J3, Size 66846720 Bytes (~64 MB)
  o IronWare Image (Primary)
    Version 6.0.0aT177, Size 9529041 bytes, Check Sum a2c5
    Compiled on Jul 25 2016 at 11:27:22 labeled as xmlp06000a
  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 = 2.05, Build Time = 5/20/2015 22:20:00

 XPP Version = 6.14 (NPB), Build Time = 5/18/2016 17:39:00

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
All show flash done
MLX-GVR#
```

Output example for the show module command

```
MLX-GVR#show module
90
Module                                                    Status
Ports    Starting MAC
M1 (upper):BR-MLX-MR2-X Management Module                 Active
M2 (lower):BR-MLX-MR2-X Management Module                 Standby(Ready State)
F1: NI-X-HSF Switch Fabric Module                         Active
F2: NI-X-HSF Switch Fabric Module                         Active
F3: NI-X-HSF Switch Fabric Module                         Active
F4:
S1: BR-MLX-10Gx20 20-port 1/10GbE Module                  CARD_STATE_UP
20       cc4e.2445.2300
S2: BR-MLX-100Gx2-CFP2 2-port 100GbE Module               CARD_STATE_UP
2        cc4e.2445.2330
...
...
...
```

```
S15: BR-MLX-100Gx2-CFP2 2-port 100GbE Module                    CARD_STATE_UP
2        cc4e.2445.25a0
S16: BR-MLX-10Gx20 20-port 1/10GbE Module                       CARD_STATE_UP
20       cc4e.2445.25d0
MLX-GVR#
```

OpenFlow upgrade and downgrade

When downgrading the system from R06.0.00a 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.

Brocade 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 Brocade NetIron Software Upgrade Guide.

Hitless upgrade support

Hitless Upgrade from any release to R06.0.00a is NOT supported.

Limitations and restrictions

Compatibility and interoperability

- Mlxe (NI6.0) and Vyatta (4.2R1) IPsec interop
- Mlxe (NI5.9.0a) and ICX (8.0.41) IPsec interop
- Mlxe (NI6.0) and BFO 1.2 interop

802.1BR and VN-tag header processing have the following limitations.

- If the ingress port is on a 24x10 module, it is recommended to use a catch all Layer 2 Policy Based Routing (L2 PBR) to forward that traffic to a service port for VNTAG and 802.1BR header removal, followed by L2 and L3 PBR on the service port.
- Other ingress modules (8X10G etc) can separate the 802.1BR and VNTAG traffic to the service port using L2 PBR, and conduct L2/L3 PBR matching on the remaining traffic.
- 802.1BR header stripping and VN-tag header stripping features are supported in BR-MLX-40Gx4, BR-MLX-10Gx20, and BR-MLX-100Gx2-CFP2 modules.
- When using the 802.1BR header stripping and VN-tag header stripping features with loopback system configuration (intermediate card), support is only available on the BR-MLX-40Gx4 module. The 802.1BR header stripping and VN-tag header stripping configuration with loopback system is not supported on the BR-MLX-10Gx20 and BR-MLX-100Gx2-CFP2 modules.

Important notes

Brocade NetIron CES device (512M memory) recommendations.

- Brocade NetIron CES configured with any MPLS feature AND any Layer 2 or Layer 3 scalability running at maximum system values will run at borderline or below the threshold memory for normal runtime operation. This is NOT a recommended configuration in NetIron 6.0.00x. Customers on earlier NetIron versions should not upgrade to NetIron 6.0.00x.
- Brocade NetIron CES configured with any MPLS feature and any Layer 2 or Layer 3 scalability running at default system values will run above threshold memory for normal runtime operation. This is a supported configuration for NetIron 6.0.00x.
- Brocade NetIron CES configured with any Layer 2 or Layer 3 scalability running at maximum system values and without any MPLS feature will run above threshold memory for normal runtime operation. This is a supported configuration for NetIron 6.0.00x.
- MCT timers for CES/CER: Recommended timers for scaled environments are 1s for 3 tries.
- BFD for CES/CER: In highly scaled CES/CER environments, the implementation of BFD is not recommended.
- IPSec and Hitless Upgrade: A few IPsec tunnels may flap during HLOS window for certain highly scaled scenarios with short rekey timers.

Optics adapters

- The NetIron 6.0.00a release includes support for the CFP2-TO-QSFP28-MOD optics adapter. Upon installation, expect a linkup time of approximately 10 seconds.

Hardware Notes

MR management module is supported until R05.7.00, and not supported in NI R05.8.00 and later.
The MR2 management module is required in NI R05.8.00 and later releases.

- If Gen1.1 line cards are present in a chassis, Gen3 modules cannot go to –X2 scale. In such cases, only the scale defined for Gen1.1 cards can be achieved. Gen1.1 cards will have to be removed from the chassis to achieve –X2 scale.
- On a chassis with Gen1.1 cards, it is strongly recommended to keep system-max values within the maximum supported in the CAM profile being used.
- With 1.8M IPv6 routes, during an MP switchover, protocol flaps or ND flaps could be encountered. The workaround is to use the following timer configuration –

```
ipv6 nd reachable-time 3000
!
!
!
address-family ipv6 unicast
graceful-restart restart-time 1800
graceful-restart stale-routes-time 1900
graceful-restart purge-time 1950
```

- With –X2 scaling, it is recommended to limit BFD timers to >= 200ms using the command -
  - `bfd interval 200 min-rx 200 multiplier 3`
- With 2.4M IPv4 routes, BGP can take 3 to 4 minutes to learn routes on MP and 10 to 15 minutes to program routes on the LP. If the routes have MPLS next hops with several ECMP paths, learning can take up to 25 minutes.
- With 2M VPN routes configured, deleting 1000 VRFs or more within a few seconds might result in the MP and LP being out-of-sync. Workaround would be to leave a 5 second gap between deletion of every VRF.
- With –X2 scaling, LACP (short timer) flaps may be seen when an LP on which 2.4M IPv4 routes have been learned is reloaded.
- On BR-MLX-10Gx4-M-IPSEC, in 1G mode, when unencrypted traffic exceeds 99.9%, `InErrors`, may be seen in the "`show statistics`" output. These are seen as FCS errors (as shown below). This issue can be seen on the four 1G ports, as well as the four 10G/1G ports when operating in 1G mode, with non- IPsec traffic.
- 100% throughput can be achieved on BR-MLX-10Gx4-M-IPSEC with IPsec traffic.

```
Router#sh st e 1/6

PORT 1/6 Counters:
         InOctets         7831740944          OutOctets         7831962000
           InPkts             870257            OutPkts             870218
  InBroadcastPkts                  0    OutBroadcastPkts                  0
  InMulticastPkts                  0    OutMulticastPkts                  0
    InUnicastPkts             870131      OutUnicastPkts             870218
       InDiscards                  0         OutDiscards                  0
         InErrors                126           OutErrors                  0
     InCollisions                  0       OutCollisions                  0
                                       OutLateCollisions                  0
        Alignment                  0                  FCS                126
  InFlowCtrlPkts                   0     OutFlowCtrlPkts                  0
        GiantPkts                  0           ShortPkts                  0
     InBitsPerSec          997746326       OutBitsPerSec          997737206
     InPktsPerSec              13859       OutPktsPerSec              13857
    InUtilization             99.99%      OutUtilization             99.99%
```

- 100G CFP2 ER4 optic is supported on the MLXe 2-port 100GbE CFP2 line card with hardware revision 15 or later only. Use the *show version slot* command to check the hardware version of the line card and confirm that the part number (underlined in the example below) is -15 or later.

Syntax: **show version slot** <*slot number*>

```
MLX#sh ver sl 4
==========================================================================
SL 4: BR-MLX-100Gx2-CFP2 2-port 100GbE Module (Serial #: CWC0440K027, Part #:
60-1002934-15)
License: 2x100GbE-X2-Scaling-UPG (LID: eyeFJJFmFHM)
Boot     : Version 5.9.0T175 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900
 (449576 bytes) from boot flash
Monitor  : Version 5.9.0T175 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Mar 19 2015 at 03:17:18 labeled as xmlb05900
 (568786 bytes) from code flash
IronWare : Version 5.9.0pT177 Copyright (c) 1996-2015 Brocade Communications
Systems, Inc.
Compiled on Nov 18 2015 at 17:02:00 labeled as xmlp05900p112
 (9481314 bytes) from Primary
FPGA versions:
Valid PBIF Version = 2.05, Build Time = 5/20/2015 22:20:00

Valid XPP Version = 4.05, Build Time = 11/4/2015 13:51:00

MACXPP100G 0
MACXPP100G 1
1199 MHz MPC P2010 (version 8021/1051) 599 MHz bus
512 KB Boot Flash (MX29LV040C), 66846720 Bytes (~64 MB) Code Flash (MT28F256J3)
3072 MB DRAM, 8 KB SRAM, 286331153 Bytes (~274 MB) BRAM
LP Slot 4 uptime is 19 days 1 minutes 57 seconds
```

TSBs

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 http://my.brocade.com under the "*Technical Documentation*" section of the "*documentation*" tab (note that TSBs are generated for all Brocade platforms and products, so not all TSBs apply to this release).

TSB issues resolved in 6.0

TSB	Summary
TSB 2016-232-A [1}	When upgrading to NetIron 5.7.00 or later from any version prior to NetIron 5.7.00, any ACL with a name starting with a number will not be applied after reload.
TSB 2016-233-A	With the default configuration, in 5.8.00d the MAC Port Security feature does not block non-secure MACs.
TSB 2015-212-A [1]	This concerns a vulnerability in the Network Time Protocol (NTP) Project NTP daemon (ntpd) documented by CVE-2014-9296. The ntpd version 4.2.7 and previous versions allow attackers to overflow several buffers in a way that may allow malicious code to be executed. The NTP Project daemon implementation is widely used in operating system distributions and network products. This vulnerability affects ntpd acting as a server or client on a system in which not only is authentication configured, but an authentication error occurs.

Defects

Closed with code changes R06.0.00a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 8/11/2016 in NI 6.0.00a. This list was updated on 06/20/17.

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 the interface 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 remote end was removed. 2. When the remote end device is Infinera WDM/DTN-X device	
Recovery: Remove and Re-insert of the TX cable from the remote end.	

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 the BGP operation and starts again	

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: Happens on a scaled scenario on a slow server with a response time more than 10 seconds. No path is available for the LSPs, so the LSPs keep retrying.	
Condition: 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. 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: 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: 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: 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: DEFECT000594318	
Technical Severity: High	**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: 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: 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: 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: 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: 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: 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: DEFECT000599114	
Technical Severity: High	**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: 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: 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: Observe 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: 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: DEFECT000600734	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** LAG - Link Aggregation Group
Symptom: Secondary port in a LAG remains in LACP-BLOCKED state after removing it and re-adding it in a LAG that has "force-primary-port-mac" enabled.	
Condition: LAG configuration should have "force-primary-port-mac" enabled. L2ACL used on the primary port should have a permit rule only for primary port of the peer LAG. Ex: If primary port MAC of the peer is aaaa.bbbb.cccc the L2 ACL should be : mac access-list acl_sample permit aaaa.bbbb.cccc ffff.ffff.ffff any any etype any deny any any any etype any	
Workaround: Add the interface MAC of all the member ports of the LAG to the L2ACL	
Recovery: Add the interface MAC of the current primary port of the LAG to the L2ACL if there is a change in the primary port status	

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: 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: 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: 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: 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: 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: 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: 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: 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: When SNMP polling of 100Gx2-CFP2 optics OR CFP2 to QSFP28 adapter, the Management module may unexpectedly reload and switchover 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: 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: 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 disable and enable interface having CFP2 SR10 or QSFP28 transceiver modules.	
Condition: This issue is specific to QSFP28 and CFP2 SR10.	

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	

Closed with code changes R06.0.00

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 4/25/2016 in NI 6.0.00. This list was updated 5/26/16.

Defect ID: DEFECT000534315	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** Configuration Fundamentals
Symptom: MLX8x10 line cards may fail initialization in a chassis with scaled configurations with the following reason code seen in "show module" output. CARD_STATE_DOWN(22) .. Card State Down Reason Code: 22 CARD_DOWN_REASON_TM_LBG_TEST_FAIL	
Condition: Certain scaled scenarios and multiple line cards powering up at the same time may cause the issue.	
Recovery: Power cycle the line card.	

Defect ID: DEFECT000544399	
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: Error message "free_config_buffer: bad buffer address: 28310000 20335b90 20335fb0 209f1c2c 20ae38fc 20ae3c34 209e98e8 00005e18 00000000" may be seen after successful config file transfer with tftp via ssh.	
Condition: Executing transfer of config file via tftp over SSH. .	

Defect ID: DEFECT000551250	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** IP Addressing
Symptom: CER configured as DHCP relay agent does not forward the DHCP offer.	
Condition: 1) From CER the reachability to another DHCP server/relay agent should be set up via static route under VRF with VE interface. 2) Unconfigure and reconfigure the VE interface.	
Recovery: Unconfigure and reconfigure the static route that points to the DHCP server/ relay agent.	

Defect ID: DEFECT000552823	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** OAM - Operations, Admin & Maintenance
Symptom: Remote-fault will not work for the ports of 20x10GE and 4x10GE-IPSEC line card modules.	
Condition: Applicable for ports of 20x10GE and 4x10GE-IPSEC line card modules.	

Defect ID: DEFECT000555532	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPSec tunnel flaps may be observed and related SysLogs are generated.	
Condition: May happen in a scaled scenario with both IPSec and sFlow configuration on an IPSec interface.	

Defect ID: DEFECT000557149	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: Warning message "ITC_MSG_TYPE_HAL_RESPONSE (00130094) received for app 0000003f" may be seen.	
Condition: When using an OpenFlow 1.3 controller to administrate OpenFlow port up/down state.	

Defect ID: DEFECT000558739	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: IPv4 MTU gets cleared despite throwing an error message while executing the command "no ip mtu <value>"	
Condition: 1. Support for Jumbo frames should be enabled 2. Configure IPv4 MTU to be greater than 1500 bytes 3. Configure GRE Tunnel MTU to be greater than default Maximum value (1476)	
Workaround: The GRE Tunnel MTU can be re-configured after removing the IPv4 MTU (OR) Remove the GRE Tunnel MTU configuration before modifying IPv4 MTU	

Defect ID: DEFECT000558932	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.8.00	**Technology:** OpenStack Integration
Symptom: Continuous reload of line card module	
Condition: Source path having invalid FPGA image	
Recovery: Place the correct image in the source path and retry the line card module auto upgrade procedure	

Defect ID: DEFECT000559099	
Technical Severity: Medium	**Probability:** High
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: 6PE and 6VPE may not work for a certain range of BGP nexthop addresses. If any of the higher two octets of the nexthop address is 255, then these nexthops will not be reachable.	
Condition: In 6PE and 6VPE deployment if the BGP nexthop address used is of range where any of the higher two octets is 255 in the IPv4 address part of the IPv4 mapped IPv6 address, this nexthop address and the BGP routes with that nexthop address will not be reachable. For example, if the BGP nexthop for 6PE or 6VPE is :FFFF:X.X.Y.Y (IPv4 mapped IPv6 address), and if X is set to 255, then those nexthop addresses might not be reachable in BGP.	
Workaround: Use address in a different range as BGP nexthop address.	
Recovery: Issue clear ip bgp neighbor <x.x.x.x> or clear ip bgp vpnv6 neighbor <x.x.x.x>, where <x.x.x.x> represents 6PE or 6VPE neighbor.	

Defect ID: DEFECT000559396	
Technical Severity: Low	**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: 1) Same destination learnt from multiple ASBRs is shown as OSPF ECMP route in routing table. 2) Same destination learnt from multiple ASBRs (at least one of them in a NSSA area), only the non-NSSA route is shown in the routing table.	
Condition: Routes learnt by ABRs in the following cases: - 1) Same destination advertised by ASBRs present in multiple areas with at least one of them in the backbone area. 2) Same destination advertised by ASBRs present in multiple areas with at least one of them configured as NSSA.	

Defect ID: DEFECT000559995	
Technical Severity: Medium	**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: Unexpected reload of Management module in BGP task	
Condition: When BGP receives route updates with duplicate community from peer and either of the following conditions occur: - 1) Route map processing is done for the received duplicate community 2) The following command is executed show ip bgp routes detail x.x.x.x	

Defect ID: DEFECT000560809	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: Unexpected reload of Management Module.	
Condition: 1. "static-network" should be configured under BGP 2. BGP peer announcing the route, which is same as the configured static network.	
Workaround: Have a route-map configured that will deny routes from peers that are matching with the static-network configured.	

Defect ID: DEFECT000560832	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.8.00	**Technology:** QoS - Quality of Service
Symptom: Throughput issues and packet loss when chassis is reloaded multiple times.	
Condition: Packets getting dropped in traffic manager. It happens for all line card types.	

Defect ID: DEFECT000561519	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: Disable/Enable of OpenFlow port from controller fails for certain conditions when the controller is connected through the management port.	
Condition: When the controller is connected via the management port and - is trying to enable/disable OpenFlow port 1/1 - is trying to enable/disable OpenFlow hybrid port and this port is part of a VE.	
Workaround: For VE port, assign the global VE MAC to the MAC address of a physical port other than port 1/1.	

Defect ID: DEFECT000561715	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** ACLs - Access Control Lists
Symptom: Accounting of Layer 2 Policy based routing will not work after hitless upgrade.	
Condition: It happens when hitless upgrade is done.	
Recovery: Need to reset the line card module to recover from this issue.	

Defect ID: DEFECT000561919	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.7.00	**Technology:** Configuration Fundamentals
Symptom: Traffic loss was seen and all the traffic was showing as dropped on NP on a 4x10G module. Port 6/1 RX NP Rx Raw Good Packet = (84418766) NP Rx Forward Packet = (0) NP Rx Discard Packet = (84418766)	
Condition: The issue appeared after line card went into rolling reboot.	

Defect ID: DEFECT000562196	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** ARP - Address Resolution Protocol
Symptom: On CER/CES, packets forwarded by HW using a static route to a /32 destination may be lost	
Condition: This issue is applicable only for CER/CES platforms (1) Static route configured to reach a /32 destination with nexthop set to one of the VE interfaces (2) Traffic to the destination should have been forwarded for some time, stopped and then resumed after a gap of at least one minute	
Recovery: "clear ip route x.x.x.x/x" for the affected route	

Defect ID: DEFECT000562309	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.2.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: BGP (peer) flap on CER devices.	
Condition: When system up time is more than 1242 days	

Defect ID: DEFECT000562467	
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: Downstream devices connected on CEP port may not receive multicast traffic from an MCT peer when the uplink connecting to the Multicast Source goes down.	
Condition: - MCT peers are CER/CES devices, and - uplink connecting to the Multicast Source and the MCT ICL on which the joins are received are on the same VLAN/VE	
Workaround: Use separate VLANs for ICL and uplink CCEP port	
Recovery: "clear ip pim mcache" on the MCT peer which is currently receiving traffic from CCEP uplink port.	

Defect ID: DEFECT000562937	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** IPv4 Multicast Routing
Symptom: "TM EGQ Discards" counters are being incremented in the egress Traffic Manager.	
Condition: Reception of multicast traffic from a directly connected source for which no listeners are present.	

Defect ID: DEFECT000562974	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** 802.1x Port-based Authentication
Symptom: If a MAC gets blocked on a PMS enabled port, packets coming from the same MAC on a non-PMS enabled port will not result in source MAC being learned.	
Condition: - Topology that has possibility of loop formation - Mixture of PMS and non PMS enabled ports	

Defect ID: DEFECT000563075	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.6.00	**Technology:** OpenStack Integration
Symptom: MBridge copy failure with error message "Failed to write to destination file" may be seen.	
Condition: This happens when the MBridge FPGA image is copied more than once without a reload between the copy operations, if there is not enough space in flash to accommodate multiple MBridge files.	
Workaround: Leave enough space in flash before copying the image/FPGA	
Recovery: Delete the '__mbridge.old' file as shown below and then copy the MBridge file - Router#del ___mbridge.old	

Defect ID: DEFECT000563167	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** IP Addressing
Symptom: The command "show vlan ethernet <slot/port>" does not show the secondary port of a LAG configured under a VLL VLAN.	
Condition: LAG port should be configured to be a part of a VLL VLAN.	

Defect ID: DEFECT000563199	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** LAG - Link Aggregation Group
Symptom: Port on a 8x10G Line card module may sometime not recover after it goes down with a local fault	
Condition: When Lockup condition on PHY occurs for a port on an 8x10G Line card module.	
Recovery: Only power cycle of the affected Line card module can recover the condition	

Defect ID: DEFECT000563429	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: Reachability issues if client interface is shutdown on both MCT peers and then enabled back on one of the MCT peers.	
Condition: This issue will happen only when the client-interface shutdown is done on both MCT peers and enabled back on one of them.	
Workaround: Avoid shutting down clients on both MCT peers.	
Recovery: Enable client interfaces on both MCT peers and then the peers would be reachable.	

Defect ID: DEFECT000563461	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** VRRPv3 - Virtual Router Redundancy Protocol Version 3
Symptom: Error messages "ITC_ERR_DEST_QUEUE_FULL" may be seen on the management module console, and some Line card modules reload automatically and do not come up again.	
Condition: This may happen if the system has a highly scaled configuration with a lot of VPLS VPorts, VRRP-e instances, ARP entries, and VPLS MAC address in the MCT environment.	
Recovery: Reload the Line card modules one at a time.	

Defect ID: DEFECT000563527	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.4.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: With disable/enable of CCEP in MCT, BUM Traffic may get dropped intermittently (or loop) for LACP transition duration.	
Condition: MCT client flap.	
Workaround: Issue recovers automatically in a few seconds, and this issue may be seen only during transition time.	

Defect ID: DEFECT000563742	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** SSH - Secure Shell
Symptom: "Bad client version string" error is reported when backing up MLX configuration via SCP through BNA.	
Condition: This error is seen only when SSH Client uses a version string that has more than 65 Characters.	

Defect ID: DEFECT000563854	
Technical Severity: Medium	**Probability:** Low
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: Some OSPF routes missing from the IP routing table	
Condition: 1) CES/CER router running OSPF 2) The router 'uptime' has to be more than 1242 days	

Defect ID: DEFECT000563862	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.7.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Same VLAN is reported as Source and Destination in sFlow records when "vll-local" or "vpls-local" is configured.	
Condition: This behavior is seen in BR-MLX-10Gx24-DM module.	

Defect ID: DEFECT000564056	
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 GET query returns for unsupported objects “no such instance currently exists”.	
Condition: When ‘snmpget’ is performed on unsupported objects, it returns “no such instance” instead of returning “deprecated”.	
Workaround: These objects are not supported.	

Defect ID: DEFECT000564065	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.7.00	**Technology:** OpenStack Integration
Symptom: The port name on a LAG port may not be displayed when executing command ‘show run interface’. The port name is displayed when executing command ‘show interface’.	
Condition: Port should be a member of a LAG port.	

Defect ID: DEFECT000564079	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: Show resources indicates HW mac table usage is relentlessly increasing. MAC table size increases about 1 to 2% a day.	
Condition: The issue happens with VPLS over MCT on CER platform, when there are VPLS instance flaps in the network, causing MAC CAM leaks.	

Defect ID: DEFECT000564081	
Technical Severity: Low	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.7.00	**Technology:** OpenStack Integration
Symptom: When executing command ‘show tech’, in the following line the output contains a misspelling "statatistics" instead of statistics: BEGIN: ipc show statatistics[second time]	
Condition: Appears when executing ‘show tech’ command.	

Defect ID: DEFECT000564264	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** Static Routing (IPv4)
Symptom: After upgrade from 5600f to 5800b image, config of all vrfs with max-route configured to any value above ‘system-max ip-vrf-route" gets deleted.	
Condition: Upgrading to 5800b.	

Defect ID: DEFECT000564299	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.7.00	**Technology:** OpenStack Integration
Symptom: Complete traffic drop in egress TM on 20x10 module can be observed. This problem was seen in R5.7	
Condition: Complete traffic drop in egress TM on 20x10 module can be observed in case of flow control from egress XPP	

Defect ID: DEFECT000564387	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS VLL - Virtual Leased Line
Symptom: In CER/CES devices, CVLAN tag disappears over a VLL that is operating in Raw-mode for IPv4 packets.	
Condition: This behavior is observed when VLL raw mode with untagged endpoints and CVLAN tag type(ex:0x8100) is different from port tag type (ex: 0x9100)	
Workaround: Use VPLS or VLL tagged mode with tagged endpoints.	

Defect ID: DEFECT000564534	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast Routing
Symptom: Extra multicast traffic may be forwarded on the port that is not the part of outgoing interface.	
Condition: Hitless reload of the device without enabling nonstop routing.	
Workaround: Perform switchover command when nonstop routing is not enabled.	
Recovery: Execute "clear ip pim mc" to clear the entries.	

Defect ID: DEFECT000564675	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: ‘show tech l4 pbr’ output may not display the entire UDA PBR configuration.	
Condition: UDA PBR route map must be configured. This does not have any functional impact on the UDA PBR feature.	
Workaround: Use command “show pbr inter ethernet <port>”	

Defect ID: DEFECT000565193	
Technical Severity: Medium	**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: Traffic loss and Line card Module reset with Traffic Manager errors.	
Condition: Following logs will be observed in sys log. Jun 12 06:43:43:N:System: Module down in slot 4, reason CARD_DOWN_REASON_POWERED_OFF_SYS_MONITOR. Error Code 0 Jun 12 06:43:43:D:System: TM errors detected in slot 4 ppcr 0 Reg Offset 00002980 Value 00000004	

Defect ID: DEFECT000565259	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: BFD session at both ends may remain in DOWN state, when an LSP is configured with a detour path and low BFD timer values less than the default values, and when the LSP egress interface is disabled.	
Condition: This may occur due to certain timing scenarios where the BFD packets order causes the LSP ingress to not process the packets correctly.	

Defect ID: DEFECT000565346	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Clear IPSec SA of an IPSec tunnel may bring down the IKE SA also in a scaled set up.	
Condition: Execute 'clear ipsec sa' command	
Recovery: Systems recovers on its own.	

Defect ID: DEFECT000565392	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: CPU usage on a Line card module may go high after a Hitless software upgrade.	
Condition: Hitless upgrade.	
Recovery: System recovers after some time.	

Defect ID: DEFECT000565398	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: "show openflow flow" output may display as generic flow hardware entry consumed even after all the flows are deleted thus unable to create more flows.	
Condition: After adding MPLS label match generic flow, when any of the ports is enabled for OpenFlow hardware entries are consumed incorrectly as per "show openflow flows" counter.	
Workaround: Avoid enabling OpenFlow on ports after installing MPLS label match flows.	

Defect ID: DEFECT000565403	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.9.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Management module may unexpectedly reload when "no router mpls" command is executed.	
Condition: Router has MPLS configurations in the node with standby MP up. There must be at least one LSP in the process to be synced to the standby MP.	

Defect ID: DEFECT000565713	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Some of the IPSec Tunnels using manual certification authentication may take longer than expected to come up.	
Condition: Hitless upgrade	
Workaround: 1. Use other authentication method. 2. Clear/reset the affected tunnels.	
Recovery: Reset/clear the affected tunnel	

Defect ID: DEFECT000565828	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Telemetry
Symptom: Unable to mirror PBR next-hop invalid packets	
Condition: 1) Mirroring enabled on the port 2) PBR next hop rule should be invalid for the affected stream	

Defect ID: DEFECT000565966	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPSec Line card module reload may be seen.	
Condition: If same tunnel source and destination addresses are configured for multiple IPSec tunnels.	
Workaround: Avoid using the same source and destination addresses for multiple tunnels. This configuration is not supported.	

Defect ID: DEFECT000566294	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.9.00	**Technology:** OpenStack Integration
Symptom: When tm-voq collection feature is disabled, 'show tm-voq-stat' command should not show voq statistics. But, only for option 'show tm-voq-stat src-port' the statistics is shown even though the feature is disabled. This has been fixed. After fix, when tm-voq stats collection feature is disabled, it will throw error for all 'show tm-voq-stats' commands.	
Condition: This bug was introduced in coding for all sub options of 'show tm-voq-stat' command (queue-drops, dst-port, max-queue-depth, dst-lag), error message will be thrown when the feature is disabled. But for 'src-port' sub option alone, this validation was not added. This has been fixed.	

Defect ID: DEFECT000566312	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** GRE - Generic Routing Encapsulation
Symptom: Line card Module having GRE tunnel end point may unexpectedly reset.	
Condition: 1. GRE tunnel should be configured. 2.GRE recursive routing should happen 3. Incoming traffic MTU should be more than MTU size of GRE tunnel and hence result in fragmentation.	
Workaround: Add a static route towards the GRE tunnel end point to prevent the recursive routing.	

Defect ID: DEFECT000566498	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: IPSec log observed is success irrespective of EC key pair generation failed/passed.	
Condition: EC key generation should fail.	

Defect ID: DEFECT000566879	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.7.00	**Technology:** ACLs - Access Control Lists
Symptom: Intermittent high latency is observed for traffic such as Ping/TFTP/SSH	
Condition: This is seen when acl-accounting is enabled for more than 10,000 ACL rules.	

Defect ID: DEFECT000566985	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.4.00	**Technology:** Software Installation & Upgrade
Symptom: After an upgrade or downgrade, some Switch Fabric Modules (SFMs) fail to boot up and go to a powered off state on an MLX-32 with MR1 cards.	
Condition: During code upgrade or downgrade with SBRIDGE image copied through "manifest copy" command. Sometimes, SBRIDGE image is not copied properly to some of the Switch Fabric Modules (SFMs) even though the manifest copy command is successful.	

Defect ID: DEFECT000567391	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Salt value associated with the IPSec encryption key may be displayed as zero.	
Condition: May be seen when AES-GCM-128 algorithm is used for encryption/decryption of packets over IPSec tunnel.	

Defect ID: DEFECT000567447	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Traffic loss for High priority Open Flow rule may be seen while applying Low priority Open flow rule with the same matching criteria.	
Condition: When installing a lower priority flow with higher priority flows present, when no gaps are available in the HW CAM.	

Defect ID: DEFECT000567625	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Configuration Fundamentals
Symptom: Link remains UP and traffic passes through even though Auto Negotiation settings on 20x10G Line card Module port does not match with the remote end.	
Condition: 1) Auto Negotiation should be enabled on 20x10G Line card Module port as well as its remote end 2) Port should be UP on both ends 3) Disable Auto Negotiation on 20x10G Line card Module port	

Defect ID: DEFECT000568041	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Warning message similar to the one mentioned below is reported in optical monitoring when doing SNMP walk: - OPTICAL MONITORING: port 5/3 (4x40), failed to read latched flags when snmp polling occur	
Condition: When doing continuous SNMP polling on the following optic related OID's. snIfOpticalMonitoringInfoTable (brcdIp.1.1.3.3.6) snIfOpticalLaneMonitoringTable (brcdIp.1.1.3.3.10)	
Workaround: Increase the SNMP polling intervals.	

Defect ID: DEFECT000568140	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** Licensing
Symptom: Unexpected reload of Management module when copying license file.	
Condition: Copying of license file with file size 0 (empty file) through Tftp://ftp./	

Defect ID: DEFECT000568638	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: Link goes down without any fault notification on 2x100G-CFP2, 20x10G and 4x10G-IPSEC line cards	
Condition: For a 2x100G-CFP2/20x10G/4x10G-IPSEC line card port, local fault is not detected but remote end connected to these ports detects remote fault	

Defect ID: DEFECT000569107	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** VLAN - Virtual LAN
Symptom: By default, VLAN state of port is untagged in VLAN1. When OpenFlow hybrid feature is enabled on port, it is allowed to remove the untagged component of the port from VLAN1. When OpenFlow is disabled the ports did not revert to untagged state and would not allow user to configure it as untagged port on any VLAN.	
Condition: OpenFlow configuration.	

Defect ID: DEFECT000569387	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: Unexpected traffic loss when a Layer 2 ACL is bound to an interface with the intention of filtering based on ethertype value and priority-mapping.	
Condition: Layer 2 ACL with rule to match based on ethertype value configured as hexadecimal number and also priority-mapping value.	

Defect ID: DEFECT000569396	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: User isn't allowed to add a L2 ACL rule which contains ethertype hexadecimal value 00008902 with priority or priority-force options.	
Condition: When user tries to configure a L2ACL rule with ethertype hexadecimal value 00008902 with priority or priority-force option, an error message is displayed and the rule doesn't get added to the L2 ACL table.	

Defect ID: DEFECT000569416	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** ACLs - Access Control Lists
Symptom: System will not be able to add rule with protocol number as 58 if rule with protocol as ICMP is already configured in ipv6 filter and when duplicate-check is enabled.	
Condition: Configure ipv6 filter with protocol as ICMP and enable duplicate-check. Then try to configure new rule with protocol number as 58.	

Defect ID: DEFECT000569740	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** Configuration Fundamentals
Symptom: TIME-STAMP shows negative value in show tech-support output.	
Condition: The system up time is 248 days or above.	

Defect ID: DEFECT000569791	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Crypto key generation config will be lost after reload of the router.	
Condition: If duplicate crypto key label names are allowed.	

Defect ID: DEFECT000570174	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPsec tunnel comes up when the ESP algorithm is AES-GCM-256 and IKEv2 algorithm is AES-CBC-128.	
Condition: Configure IKEv2 algorithm as AES-CBC-128 and ESP algorithm as AES-GCM-256. IPsec tunnel should not be allowed to come up.	

Defect ID: DEFECT000570194	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** sFlow
Symptom: In CES/CER boxes, sFlow packet sampling may stop working	
Condition: When IP receive ACL is configured sFlow packet sampling may stop working.	

Defect ID: DEFECT000570596	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** VLAN - Virtual LAN
Symptom: CER/CES devices may not properly flood broadcast/unknown unicast/multicast frames	
Condition: Conflict between global and interface route-only/no route-only configuration on a dual mode / tagged interface.	
Workaround: For VLAN tagged ports ensure route-only/no route-only configuration on interface level is the same as global level configuration.	
Recovery: Change the interface level route-only/no route-only configuration for VLAN tagged ports to match the global level configuration.	

Defect ID: DEFECT000570706	
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: Router shows incorrect OSPFv3 Area Border Router status and can unexpectedly reload after the last virtual link is removed from OSPFv3	
Condition: When the last virtual link is removed from OSPFv3 and if no backbone area exists.	
Workaround: Configure a backbone area.	

Defect ID: DEFECT000570755	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Software Installation & Upgrade
Symptom: TFTP copy of NI 6.0 Management Module image fails with below error message: "Download to primary flash failed - TFTP: downgrade below v5.2 not allowed"	
Condition: (1) TFTP copy of Management Module image for upgrade from NI 5.3 and above to NI 6.0 (2) Presence of MR2 Module	
Workaround: (1) Enter OS/monitor mode on MP by pressing Ctrl+y, m (2) Copy the individual application image of NI 6.0 in monitor mode e.g., “copy tftp flash <ip_address> xmr06000b016.bin primary” (3) Reload the router (4) Then upgrade the other images, or run manifest upgrade.	

Defect ID: DEFECT000570849	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** ACLs - Access Control Lists
Symptom: IPv6 Syslog message always displays the primary port even though the denied packet has arrived on the secondary port.	
Condition: This behavior is seen when "enable-deny-logging" is enabled on the LAG or VE associated with the LAG and "deny" filter with "log" option is enabled in the ACL. In the presence of such a configuration, packets that get denied should arrive on the secondary port of LAG.	

Defect ID: DEFECT000570890	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** 802.1x Port-based Authentication
Symptom: Management module may unexpectedly reload when processing access accept message from RADIUS server.	
Condition: Reception of access accept message from RADIUS server.	

Defect ID: DEFECT000571002	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.8.00	**Technology:** Rate Limiting and Shaping
Symptom: Line card module may unexpectedly reload when "clear rate-limit counters bum" is executed on the Line card module.	
Condition: Issuing command "clear rate-limit counters bum" on the Line card module.	
Workaround: Specifically mentioning port number and corresponding VLAN ID. "clear rate-limit counters bum-drop port-id x/y vlan-id z".	

Defect ID: DEFECT000571038	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: Changes in the auto-negotiation options done when the port is in 10G mode is not getting applied when the port speed is changed to 1G later on.	
Condition: This happens in the following scenario: - Applicable for 20x10GE and 4x10GE-IPSEC line cards. - Port is in 10G speed and auto-negotiation configurations are not relevant. - Change the auto-negotiation options. - Change the port speed to 1G by changing the transceiver.	
Workaround: Change the auto-negotiation options only when port speed is 1G.	

Defect ID: DEFECT000571042	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** RFN - Remote Fault Notification
Symptom: For 20x10G ports, link-fault-signaling is not working after reload.	
Condition: 1) link-fault-signaling configured on 20x10G ports. 2) Reload OR Power OFF, Power ON of the 20x10G Line card Module.	
Recovery: Removing and re-configuring link-fault-signaling on 20x10G ports.	

Defect ID: DEFECT000571357	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.6.00	**Technology:** Rate Limiting and Shaping
Symptom: After rate-limit is applied on an interface, if CIR value is changed to a value higher than the line rate for that interface, the configuration change will be accepted and the CIR value will be adjusted internally to the maximum line rate. But this causes 2 issues. 1. "no rate-limit" command will be rejected with the error message - "Error: Maximum burst is more than maximum port rate". 2. After reload, the configuration application will fail.	
Condition: Apply rate-limit on an interface and then modify the CIR value higher than the line rate for that interface	
Workaround: Ensure that the CIR value being configured in the "rate-limit" command is lower than the line rate for that interface	
Recovery: To recover after reload, re-apply the rate-limit configuration on the interface.	

Defect ID: DEFECT000571407	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.8.00	**Technology:** IPv4 Multicast Routing
Symptom: On CER-RT, traffic may not be forwarded to 10G ports/OIFs for a multicast group.	
Condition: Seen only on CER-RT, when the OIFs included ports from both PPCRs of 10G ports.	
Workaround: Issue will not be seen if all OIFs for a given group are on the same PPCR.	

Defect ID: DEFECT000571646	
Technical Severity: High	**Probability:** High
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: Invalid routes may be seen in route table when inter VRF route leaking is configured.	
Condition: When inter vrf route leak is configured and route table changes in quick succession then routes which should be deleted may be left un-deleted in VRF route table.	
Recovery: Issue 'clear ip route vrf vrf-name prefix' to remove invalid routes.	

Defect ID: DEFECT000571735	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.7.00	**Technology:** ACLs - Access Control Lists
Symptom: Command "show access-list accounting ethernet <> in rate-limit" does not show counters incrementing	
Condition: When MAC ACLs are configured and rate limiting based on MAC ACLs is applied on the interface	

Defect ID: DEFECT000571931	
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: The Management module may unexpectedly reload in OSPF task during boot.	
Condition: (1) Device should be configured as NSSA ASBR/ABR. (2) Should have at least 3 NSSA areas configured. (3) Should redistribute an external destination into various NSSA areas.	

Defect ID: DEFECT000571998	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IPv6 Addressing
Symptom: High CPU utilization resulting in packet loss.	
Condition: Configuration of "ipv6 nd local-proxy" on an MCT peer.	

Defect ID: DEFECT000572323	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.4.00	**Technology:** Hardware Monitoring
Symptom: The remote end of a link shows as UP even though the local port is disabled.	
Condition: An incompatible transceiver is inserted in a port of any Line card module.	

Defect ID: DEFECT000572378	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** Configuration Fundamentals
Symptom: In CES/CER, memory usage may reach up to 99% after configuring the system-max values.	
Condition: When large system-max values are configured in CES/CER.	

Defect ID: DEFECT000572411	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: Running configuration output may incorrectly display the command "privilege vrrp-router level 5 enable" as "privilege level 5 enable".	
Condition: Configure the command, "privilege vrrp-router level x".	

Defect ID: DEFECT000572552	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.5.00	**Technology:** BGP/MPLS VPN
Symptom: Traffic destined to one of the VRF's is dropped in L3VPN.	
Condition: L3VPN needs to be configured on CER/CES which act as a PE.	

Defect ID: DEFECT000572675	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: On an interface that has PMS enabled and "violation restrict" configured, Violation Syslog message stops printing after 5 violations for the same MAC.	
Condition: PMS should be enabled on an interface and "violation restrict" configured. Interface should receive traffic from more MAC addresses than specified in the "maximum <value>" configuration. Example Configuration is as below: interface ethernet 3/1 enable port security enable violation restrict maximum 1 In the above sample configuration, a log will be generated when traffic from at least two MAC addresses is received.	

Defect ID: DEFECT000572720	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: On Provider Edge device, BGP VRF routes learnt over IBGP neighbor are not advertised to BGP VPN address-family neighbors.	
Condition: When the CE BGP VRF neighbor is configured as IBGP session.	
Workaround: Change BGP VRF neighbors from IBGP session to EBGP session.	

Defect ID: DEFECT000572729	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: CLI allows application of an ACL to a physical interface, even when the number of rules contained in the ACL is larger than the L4 CAM space. The operation is not rejected and there is no warning logged in the Syslog.	
Condition: Number of rules in ACL clause is larger than the available L4 CAM space.	

Defect ID: DEFECT000572893	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: Unicast packets get flooded when aging interval expires for a secured port.	
Condition: This issue is applicable only on CES/CER platform and happens when an aging interval is configured (as shown below) for a secured port. Aging configured globally for all secured ports - device(config)# global-port-security device(config-global-port-security)# age 10 Aging configured for a specific port - device(config)# interface ethernet 7/11 device(config-if-e100-7/11)# port security device(config-port-security-e100-7/11)# age 10	

Defect ID: DEFECT000573138	
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: Broadcast packets are not flooded out of Uplink ports on CER/CES.	
Condition: Seen when CER/CES is rebooted with Uplink-switch configuration enabled.	
Recovery: Un-configure and Re-Configure Uplink Switch configuration.	

Defect ID: DEFECT000573303	
Technical Severity: Critical	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** IP Addressing
Symptom: Line cards may reset unexpectedly or duplicate ARP entries may be seen in Line cards.	
Condition: When LAG primary port is frequently changed.	

Defect ID: DEFECT000573507	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** Multi-VRF
Symptom: Routes in a VRF lite instance not participating in L3VPN are still programmed in the L3VPN hardware table consuming VPN hardware resource.	
Condition: VRF lite configuration in the presence of L3VPN.	

Defect ID: DEFECT000573533	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** Multi-VRF
Symptom: Line card reset may be seen when adding a new port to a VRF when the system has more than 500K VRF routes.	
Condition: When more than 500K VRF routes are learned and the first port is added into a VRF on a Line card.	

Defect ID: DEFECT000573707	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Sysmon
Symptom: In "show sysmon config" command output, SLOTS column is blank for some of the monitoring features.	
Condition: Issuing "show sysmon config" command.	

Defect ID: DEFECT000573788	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.2.00	**Technology:** Syslog
Symptom: On CES/CER platform, timestamps in syslog output may become incorrect after system uptime passes 1242 days. The syslog time stamp in one instance jumped to March from August	
Condition: When the system uptime reaches 1242 days.	
Recovery: System can only be recovered by reloading the system	

Defect ID: DEFECT000574183	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: L2 VPN MACs are out of sync between 2 MCT peers. Error messages similar to the ones listed below scroll on the console - Oct 16 01:20:37.205 Call Stack [Task l2vpn]: 0x202a9ffc 0x21529a5c 0x21529b0c 0x2147b898 0x2147bb5c 0x21486e00 0x21486ee0 0x21548888 0x21565348 0x215655f0 Oct 16 01:20:37.205 VPLS: ITC error while sending log, error code 8	
Condition: Seen when an MCT peer reloaded on a setup with over 2000 VPLS instances,100,000 VPLS MACs and corresponding scale.	
Recovery: Force a re-sync by clearing the MACs of VPLS instances on the Active MCT peer, using the "clear mac vpls" command.	

Defect ID: DEFECT000574490	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: CCEP port can go to forwarding state 1 second ahead of the configured delay.	
Condition: Bring down CCEP port Bring CCEP port back UP.	

Defect ID: DEFECT000574935	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.4.00	**Technology:** Configuration Fundamentals
Symptom: Copying of configuration from PCMCIA to running configuration fails with "invalid input" message for ACLs.	
Condition: Presence of ACL in the configuration stored in PCMCIA.	

Defect ID: DEFECT000575002	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.2.00	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: OSPF will see neighbors flap with md5 authentication failure.	
Condition: OSPF interface(s) should have md5 authentication enabled and the local router's 'uptime' has crossed 1242 days.	

Defect ID: DEFECT000575072	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Hardware Monitoring
Symptom: Remote and local fault message in syslog could be associated with a number as below. Oct 20 19:44:47:I:SYSTEM: port 4/2 is down(remote fault 1) Oct 20 19:36:18:I:SYSTEM: port 6/16 is down(remote fault 3)	
Condition: When local or remote fault is logged in syslog. Note: These numbers are used by the device for internal purposes and are not a cause for concern	

Defect ID: DEFECT000575097	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPsec tunnel between strongswan IPsec server and MLXe will not come up using certificate based signature.	
Condition: If certificate based auth method is used between MLX and another vendor, the IPSEC tunnel will not come up because AUTH Payload was sent in DER format.	
Recovery: Use PSK as auth method between MLX and another vendor.	

Defect ID: DEFECT000575273	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** CLI - Command Line Interface
Symptom: - "dir" command from the management card fails with the following error "error: File not found". - "wr mem" command from the management card fails with the error - "Write startup-config failed".	
Condition: This issue may occur if "show tech-support" command is repeatedly executed through script.	
Recovery: Reload of the router is the only recovery option	

Defect ID: DEFECT000575349	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.7.00	**Technology:** Software Installation & Upgrade
Symptom: Line card module goes to interactive state and "show module" command output displays any other reason code than "None" such as, “FPGA mismatch/monitor mismatch.”.	
Condition: 1) When any slot in the chassis has already reported a card interactive state with a reason code other than "None" 2) When any Line card module is put in the same slot and booted to interactive mode manually by the command "lp boot sys interactive <slot-no>", the card will be moved to interactive with the old interactive reason, as "FPGA mismatch/monitor mismatch.” Note: This is a display issue only.	

Defect ID: DEFECT000575361	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.8.00	**Technology:** QoS - Quality of Service
Symptom: LAG deployment will fail with following message: "QoS configuration mismatch between primary and secondary ports!"	
Condition: One of the LAG member ports belongs to a Line card Module which is configured, but not physically inserted.	
Workaround: Use command "qos multicast shaper best-effort/guaranteed rate" to apply primary port shaper values on the ports of the Line card Module that is not physically present. "Note: Shaper values of the primary port can be obtained from "show qos multicast e x/y "	

Defect ID: DEFECT000575599	
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: LAG flaps after Active to Standby MP switchover	
Condition: When Active to Standby MP switchover happens.	

Defect ID: DEFECT000575718	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Syslog
Symptom: Port will flap once and if Link Fault Signaling is enabled it will report an incorrect local fault notification before it comes up. Messages similar to the following would be SYSLOGGED. SYSLOG: <14>Oct 28 13:17:12 Router PORT: 3/1 enabled by operator from console session. SYSLOG: <14>Oct 28 13:17:12 Router System: Interface ethernet 3/1, state up SYSLOG: <14>Oct 28 13:17:13 Router SYSTEM: port 3/1 is down(local fault 1) SYSLOG: <14>Oct 28 13:17:13 Router System: Interface ethernet 3/1, state down - local fault SYSLOG: <14>Oct 28 13:17:13 Router System: Interface ethernet 3/1, state up	
Condition: When an admin disabled port is enabled and the port has LR and ER range of QSFP28 and CFP2 optics.	

Defect ID: DEFECT000575726	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Syslog
Symptom: Port will flap once and if Link Fault Signaling is enabled it will report an incorrect remote fault notification before it comes up. Messages similar to the following would be SYSLOGGED. SYSLOG: <14>Oct 28 18:39:42 Router System: Interface ethernet 3/2, state up SYSLOG: <14>Oct 28 18:39:55 Router SYSTEM: port 3/2 is down(remote fault 1) SYSLOG: <14>Oct 28 18:39:55 Router System: Interface ethernet 3/2, state down - remote fault SYSLOG: <14>Oct 28 18:39:55 Router System: Interface ethernet 3/2, state up	
Condition: When a remote port that is admin disabled gets enabled and the port has LR and ER range of QSFP28 and CFP2 optics.	

Defect ID: DEFECT000575856	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Unexpected system reload during OpenFlow 1.0 flow-stats request message processing.	
Condition: OpenFlow 1.0 flow-stats request received with match condition that matches more than 10 flows.	

Defect ID: DEFECT000575924	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** Software Installation & Upgrade
Symptom: Simplified image upgrade summary reports Line card Module monitor image installed on all Line card Modules successfully even though monitor image did not download to a few Line card Modules.	
Condition: Simplified image upgrade when LP CPU utilization is 10% or more	
Recovery: Perform the simplified image upgrade again after reducing the LP CPU utilization.	

Defect ID: DEFECT000575991	
Technical Severity: Medium	**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: Traffic loss may be observed when GRE is used with PBR	
Condition: Packets which are processed by route-map/policy-map and have their next-hop set to GRE tunnel. The incoming packet's ingress MTU should be greater than the egress tunnel MTU.	

Defect ID: DEFECT000576041	
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: In CES/CER, MCT CCP state starts to flap indefinitely when "no client-interface shutdown" command option is enabled	
Condition: MCT L2VPN configured with default L2VPN keep-alive/hold-time	
Recovery: On both ends of the MCT cluster, configure L2VPN keep-alive/hold-time to a minimum value of 600/1800 and then re-deploy the cluster. Example: "l2vpn-peer <ip> timers keep-alive 600 hold-time 1800"	

Defect ID: DEFECT000576079	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IKE session does not come up when using a certificate for authentication.	
Condition: When using IKE AUTH method as ECDSA, sometimes the IKE session does not come up.	
Workaround: Use Preshared key as IKE AUTH method to avoid this issue.	
Recovery: Clear ike sa	

Defect ID: DEFECT000576121	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.7.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP Object "ifAlias" does not display any LSP information	
Condition: 1) MPLS is enabled 2) LSP configuration should be present	

Defect ID: DEFECT000576189	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.6.00	**Technology:** OpenStack Integration
Symptom: After doing switch over, observed "fe_update_sync_err_handler:FE200: status = 7" and "Warn:rw_program_multicast_table_entry: Sync to standby MP failed for FE entry 26 (001a) (err = Timeout)" messages seen on different runs.	
Condition: During switchover on a fully loaded MLXe-32 chassis with all hSFMs and standby MP present.	

Defect ID: DEFECT000576198	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** VLAN - Virtual LAN
Symptom: ITC error messages seen on the console (with no functional impact) - Error:hal_send_itc_request: itc_send_request() failed (ret = 8) app id 00000013 Oct 30 00:56:03.169 SAT Error: itc_rw2_fe600_serdes_config - itc_send_request() failed slot:25 itc_ret:8 Oct 30 00:56:03.169 The caller task: scp had an ITC_ERROR:8Oct 30 00:56:03.169 SAT Error:	
Condition: These messages are seen after LP hot upgrade during Hitless Upgrade of an MLX/MLXe.	

Defect ID: DEFECT000576238	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: Following two symptoms are seen in CER/CES. 1) With Port security configuration on a port, when there is MAC movement from Secure port to Non-secure port, packets are flooded. 2) When the same MAC address returns to the original Secure Port, packets get dropped.	
Condition: 1) Port security is configured on a port on CER/CES. 2) MAC movement happens between a secure port and a non secure port.	
Recovery: Delete and add port security configuration again (OR) Delete the port security MAC address from running configuration.	

Defect ID: DEFECT000576302	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: MCT VPLS instances are down with the reason “wait for local functional ports”, but the associated VPLS configured ports are up. There is no functional impact.	
Condition: Seen after executing "client-interface shut" followed by "no client-interface shut", "no deploy" and "deploy" of the client.	

Defect ID: DEFECT000576487	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: After doing MCT Cluster "no deploy", the peer CCP is down with inappropriate reason "Invalid Application packet received message came from peer.	
Condition: MCT Cluster "no deploy"	

Defect ID: DEFECT000576744	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** MBGP - Multiprotocol Border Gateway Protocol
Symptom: Upon modification of any VRF attributes like route-target or route-map VRF routes that were earlier not advertised to VPN neighbors would never be advertised even if the route-target or route-map allows for such advertisement.	
Condition: When BGP VPN neighbor is established and local VRF routes are added before configuring export route target, and later export route target is added then VRF routes would not be advertised to BGP VPN neighbors.	
Workaround: Always configure export route-target in VRF before learning adding/learning routes in VRF.	
Recovery: Add VRF export route-target and clear BGP VPNv4 session.	

Defect ID: DEFECT000576778	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** Configuration Fundamentals
Symptom: Management module may reload unexpectedly or may switchover if standby management module is available. The stacktrace will show "EXCEPTION 0300, Data Storage Interrupt" at "Task: scp", but the "Possible Stack Trace" will be blank.	
Condition: This issue is seen when disabling all the interfaces of a 20x10G Line card module.	

Defect ID: DEFECT000576811	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.8.00	**Technology:** OpenStack Integration
Symptom: "flow-control rx-pause-ignore" command is not honored for 20x10G line card. Even with the command configured, unicast traffic will not be forwarded on 20x10G LP's ports when PAUSE frames are received.	
Condition: 1. The command “flow-control rx-pause-ignore” should be enabled on the interface. 2. 20x10G interface receives simple unicast traffic and pause frames	

Defect ID: DEFECT000576858	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: CCR MACs on MCT L2VPN peer not learning as CCL MACs	
Condition: When Spoke PW goes down between MCT L2VPN peers, the standby MCT L2VPN peer which becomes active does not learn MACs as CCL	
Recovery: clear mac vpls < >	

Defect ID: DEFECT000577024	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Syslog
Symptom: A port on the 20x10G module does not come up after the remote side flaps multiple times continuously.	
Condition: Seen only on the 20x10G module and with continuous flapping of remote side.	
Recovery: Remove and reconnect fiber locally or disable and enable the port again manually at remote or local end.	

Defect ID: DEFECT000577049	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.4.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Applying the “uplink-switch” command on a VLAN can cause high CPU on LPs when traffic flows on that VLAN	
Condition: Happens when the VLAN for which “uplink-switch” is applied has been configured as a “member-vlan” for MCT.	
Workaround: Step 1. Remove the VLAN from “member-vlan” configuration under MCT, Step 2. Apply “uplink-switch” on the VLAN, Step 3. Add the VLAN to the “member-vlan” configuration under MCT.	
Recovery: A “write mem” followed by a router reload is required to recover from the high CPU on LPs. If “uplink-switch” and “member-vlan” configurations are both present during reload, high CPU will not be seen after bootup.	

Defect ID: DEFECT000577299	
Technical Severity: Low	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: The "no export-vrf-leaked-routes" command is accepted at BGP configuration level even though it should only be executed under a specific address family. Router(config)#router bgp Router(config-bgp)#local-as 100 Router(config-bhp)#no export-vrf-leaked-routes No error message is printed and the configuration is accepted even though it will not take effect	
Condition: Configuring "no export-vrf-leaked-routes" command under "router bgp"	

Defect ID: DEFECT000577647	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Traffic loss and VPLS MACs out of sync between MCT L2VPN cluster peer.	
Condition: On CER platform, while executing "client-interface shutdown" and "no client-interface shutdown", the VPLS MACs are not synced to the MCT peer.	

Defect ID: DEFECT000577665	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** BGP4+ - IPv6 Border Gateway Protocol
Symptom: BGP4+ session does not establish with the desired source IPv6 address and always uses the first IPv6 address as the source IPv6 address when establishing the session.	
Condition: Two IPv6 addresses are configured on the same subnet and interface, and BGP peering is configured on second IPv6 address.	
Workaround: Under BGP configuration, use the "update source" command option to specify the desired source IPv6 address.	

Defect ID: DEFECT000577739	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: MCT CCP is kept in up state after doing "client-interface shut"	
Condition: Applying "client-interface shut" on CER-RT.	

Defect ID: DEFECT000577946	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** Hardware Monitoring
Symptom: 8x10G Line card module reports error similar to the following: - AGERAM Word 1 Parity Error on port range 1/1 - 1/4.	
Condition: There are no specific triggers for these errors. The errors will be noticed from release NI 05.6.00 onwards when the NP memory error monitoring (Line Module memory error monitoring) feature is introduced.	
Workaround: If these errors are not accompanied by traffic loss or issues in traffic forwarding, the frequency at which these errors are logged can be reduced by increasing the polling period of sysmon NP memory errors using the CLI command (from the CONFIG level), "sysmon np memory-errors polling-period <polling-period in seconds>" The default polling period is 60 seconds. It can be increased from the current default to a higher value, say 43200 seconds (every 12 hours).	

Defect ID: DEFECT000578003	
Technical Severity: Medium	**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: OSPF Summary routes and external routes will not be calculated and populated in the OSPF routing table.	
Condition: This happens when OSPF ABR and ASBR routes are filtered using a distribute-list.	

Defect ID: DEFECT000578059	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Multicast traffic loss maybe seen when multicast traffic is received on MCT CCEP port.	
Condition: When multicast traffic is incoming on a MCT CCEP port and the CCEP port flaps or goes down and traffic is moved on to other CCEP port on MCT peer.	
Recovery: clear ip pim mcache on MCT nodes.	

Defect ID: DEFECT000578298	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: System reboot may be observed with IPsec configuration.	
Condition: Issue may be observed when longer local identifier is specified under IKEv2 profile.	

Defect ID: DEFECT000578595	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Local VPLS MACs not aging out	
Condition: Disable multiple CCEP ports of MCT L2VPN at same time.	

Defect ID: DEFECT000578904	
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: Neighboring nodes of CES/CER may report protocol flaps for time sensitive protocols like LACP, BFD and may not stabilize.	
Condition: The issue can occur when there are CES/CER nodes on the network that have many instances of protocols with short timeout values configured (BFD – 15+ sessions/500 msec timeout, LACP – 5 or more with short timeout).	

Defect ID: DEFECT000579013	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.1.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Rolling-reboot is seen on CES/CER with cluster configuration.	
Condition: 1) 2x10G card should be present and have cluster configuration (client-interface ethernet <slot/port>) on its interface(s) 2) 2x10G card should be removed from the node 3) Node should be reloaded Note: Issue is specific to CES/CER platform	
Workaround: Before removing the 2x10G card, delete the associated cluster configuration (client-interface ethernet <slot/port>").	
Recovery: On boot up, press "b" to enter Monitor mode. Upload the startup config using TFTP. Edit the configuration to remove the command "client-interface ethernet <slot/port>". Download the startup configuration using Tftp://ftp./ Reboot the box again.	

Defect ID: DEFECT000579084	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Multicast traffic not received when L2 upstream is MCT peer.	
Condition: When CCEP flaps and incoming changes to ICL and back to CCEP.	
Recovery: Clear ip pim mcache	

Defect ID: DEFECT000579096	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** PBR - Policy-Based Routing
Symptom: After removal of allow-all-vlan pbr from an interface, the VLAN traffic received on the interface would still get processed.	
Condition: Removal of "allow-all-vlan pbr" option from an interface.	
Recovery: Power cycle of the module after the command has been removed is the only recovery option.	

Defect ID: DEFECT000579123	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: IPv6 ACL rate-limiting accounting doesn't increment as per traffic hitting the ACL rules. But rate-limiting of traffic works fine. The problem has been fixed in R6.0.	
Condition: With IPv6 ACL based rate-limiting configured on an interface, when user executes the command "show ipv6 access-list accounting ethernet <slot/port> in rate-limit", the accounting counters don't reflect the traffic hitting the IPv6 ACL based rate-limiting rules.	

Defect ID: DEFECT000579525	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.6.00	**Technology:** OpenStack Integration
Symptom: "Warn: active primary sync to standby MP failed!" seen on console.	
Condition: Seen when MCT CCEP/CEP ports flapped multiple times within a few seconds.	

Defect ID: DEFECT000579759	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Traffic loss and high LP CPU conditions in MCT L2VPN configuration.	
Condition: MCT L2VPN configuration.	

Defect ID: DEFECT000579937	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** Software Installation & Upgrade
Symptom: BRAM size could sometimes be displayed as zero in "show version" command output.	
Condition: On Software version NI05200 and above for 4x10G Line card module. Note: This does not cause any issue and hence can be ignored	

Defect ID: DEFECT000579942	
Technical Severity: Critical	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** PBR - Policy-Based Routing
Symptom: When user removes IPv4 PBR, L2 PBR cam is also removed.	
Condition: L2 Policy is applied on interface.	
Workaround: Disable cam sharing or apply dummy Ipv4 PBR on that interface.	
Recovery: Disable cam sharing.	

Defect ID: DEFECT000580193	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCPv6 clients do not get assigned IPv6 addresses. When a client sends a DHCPv6 request, the MLX responds with an incorrect IPv6 source address. This causes devices that have strict checking enabled (like ASUS routers) to reject the DHCPv6 response.	
Condition: MLX acting as DHCPv6 agent.	

Defect ID: DEFECT000580360	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMPv3 groups using IPv4 standard numbered ACLs may be rejected and removed from the configuration upon reload.	
Condition: Standard numbered ACL for SNMPv3 groups are applied.	
Recovery: Reconfigure the missing SNMPv3 groups after the device has fully loaded its configuration.	

Defect ID: DEFECT000580510	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** ACLs - Access Control Lists
Symptom: CES/CER node does not respond to a trace route request	
Condition: Issue can be seen when Receive ACL is configured on the CES/CER node and "traceroute" command is executed to a destination via the CES/CER node. Note: This issue is applicable only for CES/CER platforms	

Defect ID: DEFECT000580563	
Technical Severity: Low	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** BGP4+ - IPv6 Border Gateway Protocol
Symptom: IPV4 or IPV6 prefix which gets filtered due to an inbound route-map will be flagged with "F" meaning "Filtered". For such a filtered route; the next-hop will be shown as "Not Reachable" though the next-hop can be reachable. This can mislead to troubleshoot next-hop reachability.	
Condition: For a BGP neighbor inbound route-map should be configured. The prefix filtered in the route-map can be an IPV4 prefix or IPV6 prefix.	

Defect ID: DEFECT000580685	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Router reload while continuous CCEP and CEP flaps.	
Condition: On MCT L2VPN peer, when CCEP and CEP flaps continuously.	

Defect ID: DEFECT000580810	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** VLAN - Virtual LAN
Symptom: Traffic also sent to the older ports which was part of the TVF LAG LB VLAN before.	
Condition: When the TVF LAG LB VLAN was deleted and added with new set of ports, traffic also passing through older ports.	
Recovery: Add old port of the removed TVF LAG LB VLAN again to the same TVF LAG LB VLAN and remove it. or Re-load the Line Card.	

Defect ID: DEFECT000580877	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Sysmon
Symptom: The display does not show information on slot when the command "show sysmon config" is run.	
Condition: This issue is seen when the slot information is not edited.	

Defect ID: DEFECT000580978	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** SSH - Secure Shell
Symptom: Device may unexpectedly reload during SSH access.	
Condition: When unknown SSH client is trying for the SSH access repeatedly with bad login and password.	
Workaround: You can permit or deny SSH server access to the device using ACLs. To configure an ACL that restricts SSH server access to the device, enter commands such as the following. device(config)# access-list 12 deny host 10.157.22.98 device(config)# access-list 12 deny 10.157.23.0 10.0.0.255 device(config)# access-list 12 deny 10.157.24.0/24 device(config)# access-list 12 permit any device(config)# ssh access-group 12	

Defect ID: DEFECT000581192	
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: In CER/CES, when uplink-switch settings are applied to a MCT VLAN, known unicast traffic is flooded out the ICL LAG Primary port as if they are unknown unicast.	
Condition: Uplink-switch configuration should be present on a MCT VLAN.	
Recovery: Step 1. Disable the cluster ports Step 2. Do "no deploy" for associated cluster Step 3. Do "deploy" for associated cluster	

Defect ID: DEFECT000581327	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: Errors like those shown below are reported on the console and syslog. "CAM1 Dbase Parity Error on port range 1/1 – 1/4" "CAM3 Dbase Parity Error on port range 3/1" "CAM2PRAM Word 3 Parity Error on port range 6/5 - 6/8" These errors may or may not be accompanied by traffic loss or issues in traffic forwarding.	
Condition: There are no specific trigger for these errors. The errors will be noticed from release NI 05.6.00 onwards from when the NP memory error monitoring (Line Module memory error monitoring) feature was introduced.	
Workaround: If these errors are not accompanied by traffic loss or issues in traffic forwarding, the frequency at which these errors are logged can be reduced by increasing the polling period of sysmon NP memory errors using the CLI command (from the CONFIG level), "sysmon np memory-errors polling-period <polling-period in seconds>" The default polling period is 60 seconds, it can be increased from the current default to a higher value, say 43200 seconds (every 12 hours).	

Defect ID: DEFECT000581474	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.7.00	**Technology:** ACLs - Access Control Lists
Symptom: Port membership of IPv4 ACL gets affected when IPv6-ACL is bound on VE interface For example, if 'ip access-group 100 in ethe 1/3' and 'ipv6 traffic-filter ipv6acl in' are configured on a VE in the same sequence, the "show run" command displays '"ip access-group 100 in ethe 1/1 to 1/20". But, after removing 'ipv6 traffic-filter ipv6acl in', the IPv4 ACL configuration will be seen in 'show run' as 'ip access-group 100 in'.	
Condition: This happens when an IPv6 ACL is applied and removed while an IPv4 ACL also exists on the VE.	
Workaround: Issue is not seen when IPv6 ACLs are configured before IPv4 ACLs.	
Recovery: Remove and reconfigure the IPv4 ACL after adding IPv6 ACL	

Defect ID: DEFECT000581636	
Technical Severity: Low	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** ACLs - Access Control Lists
Symptom: Syslog may display wrong Ether type information for packets that are denied due to a MAC ACL enabled on an interface. Example: LLDP (Ethertype : 000088cc) traffic could be logged as APPLETALK	
Condition: MAC ACL is enabled on an interface. Command "mac access-group enable-deny-logging" is enabled. Deny rule is configured as part of ACL with "log" option enabled. Example: interface ethe 4/2 mac access-group mac_log in mac access-group enable-deny-logging mac access-list mac_log deny any any any etype 000080f3 log deny any any any etype 000088cc log	

Defect ID: DEFECT000581903	
Technical Severity: High	**Probability:** High
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: When multiple BGP neighbors are configured, configuring "filter-change-update-delay" with "0" might put some BGP neighbors stuck in "ESTABp" state. "p" meaning Filter Group change "Pending"	
Condition: Multiple BGP neighbors should be configured. "filter-change-update-delay 0" should be configured.	

Defect ID: DEFECT000582212	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** LAG - Link Aggregation Group
Symptom: If LAG member ports flap for short time, then the traffic passing through the ports may be dropped after the port(s) come up.	
Condition: LAG configuration	

Defect ID: DEFECT000582245	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Unexpected Line card reload while adding OpenFlow rule.	
Condition: Adding an OpenFlow rule with action as Port Group.	

Defect ID: DEFECT000582287	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP client will not be able to obtain the IP address	
Condition: This issue will be seen when the node is acting as a DHCP relay agent under the following conditions: - The DHCP server and the client are in non default-VRF - Static routes are used on the DHCP relay agent to forward the DHCP messages to DHCP client and server	
Workaround: On the DHCP relay agent, to reach the DHCP server and client, inter-VRF leaking should be used instead of static routes.	

Defect ID: DEFECT000582844	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.8.00	**Technology:** Static Routing (IPv4)
Symptom: CER fails to forward the traffic for the configured static route to X.X.X.X/32 with directly connected interface as next-hop.	
Condition: (1) CER is configured with a static route to X.X.X.X/32 destination with directly connected interface as next-hop. (2) IP Traffic with IP-OPTIONs comes to CER, destined to X.X.X.X/32. (3) Stop the traffic for few minutes destined to this destination.	
Recovery: clear ip route X.X.X.X/32	

Defect ID: DEFECT000582945	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** xSTP - Spanning Tree Protocols
Symptom: CER unexpectedly reloads	
Condition: All ports enabled at same time when same traffic can reach the LP CPU through different ports	

Defect ID: DEFECT000583095	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: "Client-interface shut" on standby MCT node is not working as expected as the expectation is to being the CCP down with reason "local client interfaces disabled" and CCP has to come up when "no client-interface shut" is done. But the same is not happening.	
Condition: Using "client interface shut" and "no client interface shut" with MCT VPLS setup.	
Recovery: no deploy and deeply can recover system	

Defect ID: DEFECT000583319	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP polling on bgp4V2PeerTable (OID brcdIp.3.5.1.1.2) does not display all the BGP entries	
Condition: Multiple BGP sessions should be configured and the local IP of one of the peers should be higher than the next BGP peer entry's local IP address. Sample entries are given below to explain the behavior exhibited: - BGP peer 1 local IP address : xx.xx.xx.xx BGP peer 2 local IP address : xx.xx.xx.xx BGP peer 3 local IP address : xx.xx.xx.xx In the above example, the second BGP entry with local IP address xx.xx.xx.xx will be skipped	

Defect ID: DEFECT000583379	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MAC Port-based Authentication
Symptom: Symptom 1: When a MAC moves from a secured port to a non-secured port, packets from secure MAC address get forwarded (instead of getting dropped). Symptom 2: The Violation mode with Port MAC Security configured will default to "None" instead of "shutdown". This means that the port will not be shutdown when violation occurs and all packets will continue to get forwarded. The number of MACs learnt as secure MACs will still be limited to the maximum value configured. However, the remaining MACs will get learnt as non-secure MACs. Symptom 3: After a reload, the configured violation “maximum” limit will be reset to the default value of ‘1’.	
Condition: These issues are seen in 5.8.00bm and 5.8.00d on CES/CER platforms with the Port MAC Security feature configured.	
Workaround: For Symptom 1: When PMS configuration is required, the system must be reloaded after applying it For Symptom 2: Set Violation mode explicitly to "Shutdown" using CLI For Symptom 3: After a reload, reconfigure the "maximum" limit.	

Defect ID: DEFECT000583604	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Syslog
Symptom: A port on the 20x10G module does not come up after the remote side flaps multiple times continuously.	
Condition: Seen only on the 20x10G module accompanied by continuous flapping of the remote side.	
Recovery: Remove and reconnect fiber locally or disable and enable the port again manually at remote or local end.	

Defect ID: DEFECT000583906	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.8.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Multicast traffic loss after flapping CCEP port and clearing multicast cache in an MCT network.	
Condition: Presence of 200+ IGMP groups. Continuous CCEP port flaps in a MCT cluster along with clearing of multicast cache entries on the cluster node (on which the CCEP port is flapping)	
Recovery: Clear the multicast cache entries on both MCT peers.	

Defect ID: DEFECT000584065	
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: Layer3 multicast traffic causes high CPU usage on one of the MCT cluster devices.	
Condition: Either of the following cases occurring on the peer node of a MCT setup can trigger this condition: - - MCT peer reload - Management Module Switchover of the MCT peer - Disabling and enabling Cluster Client port [CCEP]	
Recovery: Clear the multicast cache entries on both MCT peers.	

Defect ID: DEFECT000584145	
Technical Severity: Low	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** Hardware Monitoring
Symptom: Misspelling of text "search" as "serach" in diag burn-in log. Message similar to the below will be displayed: "PORT1 CAM0 serach error 0x0 0x20 :0x5120 :0x5120 "	
Condition: diag burn-in command fails because of CAM search errors when run on a Line card Module	

Defect ID: DEFECT000584285	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.8.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: On running "diag burn-in", the below error could be seen on diagnostic failure. PORT1 CAM0 serach error 0x0 0x20 :0x5120 :0x5120 diag_ntl_entry_search error Failed	
Condition: With NI5800 and above image, when running diagnostics on Line card module types 20x10G and 2x100G-CFP2.	
Recovery: Reload the system to boot up the application since these errors will be corrected by the application software.	

Defect ID: DEFECT000584298	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 06.0.00	**Technology:** IP Addressing
Symptom: Management module may unexpectedly reload	
Condition: Scaled IPSEC configuration with more than 50 tunnels and HLOS is executed.	

Defect ID: DEFECT000584661	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.6.00	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP client will not be able to obtain the IP address.	
Condition: This issue will be seen when the device is acting as a DHCP relay agent and the DHCP server/client are in different VRFs.	
Workaround: Configure DHCP server and client in the same VRF.	

Defect ID: DEFECT000584908	
Technical Severity: High	**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 ECMP route cost calculation between shortcuts and IGP path may go wrong wherein shortcut path would be preferred incorrectly.	
Condition: This issue may be observed when "reverse-metric" command is configured under global or interface level.	

Defect ID: DEFECT000585112	
Technical Severity: Low	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: 'ifTable' does not display the LAGs entries during the SNMP walk.	
Condition: Device should have LAG configured and SNMP walk should be performed on the table 'ifTable' Note: This issue is applicable from the release 5.9 onwards	

Defect ID: DEFECT000585156	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.9.00	**Technology:** MPLS VLL - Virtual Leased Line
Symptom: Below logs keeps coming on MP console. ERROR:mplp_get_lp_data_request:Session29: requested slot mask ffffffff 80000000 is invalid for msg-type 12 ERROR:mplp_get_lp_data_request:msg-type is MPLP_MSGTYPE_SCP_INFO and scp-type is 44	
Condition: VLL-LOCAL configuration on the 32 slot MLX chassis.	

Defect ID: DEFECT000585309	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.7.00	**Technology:** IPv4 Multicast Routing
Symptom: Intermittent packet loss when PIM interface through which traffic is not received flaps.	
Condition: PIM interface flaps	

Defect ID: DEFECT000585789	
Technical Severity: High	**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: Router may unexpectedly reload in OSPF task when a neighboring third party router reloads.	
Condition: - Router should have OSPF adjacency with a third party router and should have learnt Opaque LSAs from it - The neighboring router is reloaded	

Defect ID: DEFECT000586048	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Layer3 multicast traffic causes high CPU usage on one of the MCT cluster devices.	
Condition: Either of the following cases occurring on the peer node of a MCT setup can trigger this condition: - - MCT peer reload - Management Module Switchover of the MCT peer - Disabling and enabling Cluster Client port [CCEP]	
Recovery: Clear the multicast cache entries on both MCT peers.	

Defect ID: DEFECT000586114	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** CLI - Command Line Interface
Symptom: Starting 5.7.00, named ACLs are mistakenly restricted from having names that begin with a number. Because of this, when upgrading from a lower release to 5.7.00 or above, any Named ACL with a name beginning with a number will get rejected in the reload after upgrade.	
Condition: Seen in 5.7.00 and above when named ACLs are configured to have names that begin with a number.	
Workaround: Before upgrading to any release 5.7.00 or above, ensure that all named ACLs have names that do not begin with a number.	
Recovery: If any named ACLs were not applied during upgrade, reconfigure them with names that do not begin with a number and reapply them.	

Defect ID: DEFECT000586281	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: When querying the custom MIB ‘ agIpPortCounterTable’ the octet on the member links of the LAG show the same value. However, the "show stats" output for that LAG could show different values. Example: If 1/3 and 2/3 are member ports of a LAG and only 1/3 receives traffic and 2/3 does not, both could still show the same values in their counters when custom MIB ‘ agIpPortCounterTable’ is queried.	
Condition: The LAG being queried has more than one member port	

Defect ID: DEFECT000586897	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** SSH - Secure Shell
Symptom: Unexpected reload of Management module when copying multiple L2 ACL configuration files using SCP/ Tftp://ftp./	
Condition: Repeated execution of any of the below mentioned commands on the Management module where the file has at least 1000 ACLs with each ACL having 257 filters. 1) "copy scp running-config <scp-server-ip> <file-name>" (or) 2) "copy tftp running-config <tftp-server-ip> <file-name>"	

Defect ID: DEFECT000587383	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** ACLs - Access Control Lists
Symptom: Device responds to NTP query targeted for broadcast IPv4 address	
Condition: Reception of NTP query with destination IPv4 address as broadcast	

Defect ID: DEFECT000587423	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** MACsec - Media Access Control security
Symptom: When “delete-dynamic-learn" is enabled under "global-port-security", MAC addresses learnt on a PMS enabled LAG member port do not get deleted after the corresponding interface flaps.	
Condition: Under "global-port-security", "delete-dynamic-learn" is enabled. PMS is enabled on a LAG port. MAC addresses are learnt on LAG's member ports.	
Recovery: Delete the Secure MAC address learnt on the LAG port manually.	

Defect ID: DEFECT000588340	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** ERP - Ethernet Ring Protocol
Symptom: Upon reload, CES/CER nodes will go back to ERP version '1' even though the device was configured as ERP version '2'	
Condition: "raps-default-mac" option is removed from ERP configuration (as shown in the example below) to enable ERP version '2' and the device is reloaded erp 10 no raps-default-mac	
Recovery: The command "raps-default-mac" has to be removed again after reload	

Defect ID: DEFECT000588469	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: When the line card is booted to OS, from the monitor using "boot os flash primary", after some time remote console session ends abruptly. User may see the following errors just before the session termination on the line card: TSEC: bm_get_buf() failed(2) 1 TSEC: bm_get_buf() failed(2) 2 TSEC error: Invalid buffer pointer. Count=1	
Condition: When the line card is booted to OS, from the monitor using "boot os flash primary" command.	
Workaround: No workaround	
Recovery: Reboot the line card from the management card using "power-off lp" and "power-on lp".	

Defect ID: DEFECT000589350	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Intermittent multicast traffic drops.	
Condition: Seen when a PIM enabled interface with no traffic incoming or outgoing is disabled or enabled.	

Defect ID: DEFECT000589468	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Hardware Monitoring
Symptom: Low memory warning syslog messages are observed after copying an individual FPGA-XPP image to a Line card module through SSH session	
Condition: On a device that is already utilizing high memory and is close to the low memory warning threshold	
Workaround: Perform individual FPGA XPP image copy from the console or a Telnet session OR Copy the combined LP FPGA image	

Defect ID: DEFECT000589471	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Hardware Monitoring
Symptom: When connected to LR4 CFP link won't come up.	
Condition: NA	

Defect ID: DEFECT000589895	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Slow loss of packet buffer will be observed on Line card module.	
Condition: Line card module frequently receives and reassembles fragmented IPv4 PIMv2 packets.	

Defect ID: DEFECT000590494	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** ACLs - Access Control Lists
Symptom: Unexpected traffic loss when applying ACL	
Condition: Applying numbered/named L2 ACL filter with Etype in hex and priority-mapping. Example: dut1(config)#access-list 404 permit 1234.5678.1234 ffff.ffff.ffff any 4019 etype 00008100 priority-mapping 7	
Workaround: Configure ACLs with etype as the keywords instead of hexa values dut1(config)#access-list 404 permit 1234.5678.1234 ffff.ffff.ffff any 4019 etype ipv6 priority-mapping 7	

Defect ID: DEFECT000590634	
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: Device may reload when user run script which configures and un-configures IGMPv3 version configuration on tunnels.	
Condition: Repeatedly configure/un-configure IGMPv3 version configuration on tunnel.	

Defect ID: DEFECT000591720	
Technical Severity: Medium	**Probability:** High
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: For VRF/VPNV4 routes, BGP might not honor next-hop IGP metric for selecting Best-Path, even with “next-hop-mpls follow-igp” configured.	
Condition: "next-hop-mpls follow-igp” should be configured in BGP. For a VPN learned destination, there should be more than one path, and all paths should have different next-hops with same outgoing-interface/tunnel. Flapping this outgoing-interface/tunnel will result in a Best-Path that might not have honored the next-hop igp metric.	

Defect ID: DEFECT000591822	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** CLI - Command Line Interface
Symptom: Management module stops responding to the SSH and Telnet connection requests.	
Condition: When "show tech-support" is executed and the associated SSH/Telnet session is aborted midway.	
Recovery: A switch-over of the active Management module from another existing open session or reload of the router is required to recover.	

Defect ID: DEFECT000593099	
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: ifDescr for PW3 interface in a pwEnetTable was showing an incorrect value.	
Condition: Always seen for pwEnetTable.	

Defect ID: DEFECT000593652	
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: Even after removing the NTP configuration either by issuing "no ntp" or by removing all the configured NTP servers, the output of "show clock detail" command still shows the time source as NTP.	
Condition: Either by executing command "no ntp" to unconfigure NTP or by removing all the configured NTP servers	

Defect ID: DEFECT000594078	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 06.0.00	**Technology:** PBR - Policy-Based Routing
Symptom: The PBR counters for IPv4/IPv6 are not updating when the ACL contains mix of permit and deny rules.	
Condition: Create an ACL with rules with action as permit and deny. Use this ACL in PBR. Bind the PBR on an interface. Send the traffic with matching attributes. The counters are not updating properly.	

Defect ID: DEFECT000594082	
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 statistics for ipv4 pbr are getting updated twice in CES/CER box.	
Condition: Apply IPv4 PBR on interface and send traffic with matching rule attributes. The counters can be seen updating twice.	
Recovery: This problem has been addressed in R6.0	

Closed without code changes

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 4/25/2016 in NI 6.0.00.

Defect ID: DEFECT000545288	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Issuing the command 'power-off lp all' and 'power-on lp all' may cause 8x10G modules to remain down due to "LBG failure". This can cause IPC failures and the below error messages to show on the MP console: Error:sysmon_ipc_send_config: ipc_send() failed to dest_fid 0000d003 (ret = 4) Error:dcbIpcNetIron_sendIpcBuff(): IPC send failed	
Condition: This only affects 8x10G modules.	

Defect ID: DEFECT000545537	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
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: In some scenarios, for just a few routes, re-addition of non-default routes takes more than 10ms. This has no functional impact and is applicable with algorithmic mode enabled LPs only.	
Condition: After clearing VPN neighbors status for multiple non-default VRFs at the same time, the re-addition of routes results in a few routes taking more than 10ms.	

Defect ID: DEFECT000551390	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Syslog
Symptom: The below message could be seen frequently in syslog. 23: Mar 23 07:15:19:W: Latched low Temperature warning, port 16/9 24: Latched high TX Bias Current warning, port 16/9 25: Latched low TX Bias Current warning, port 16/9 26: Latched high TX Power warning, port 16/9 27: Latched low TX Power warning, port 16/9 28: Latched low RX Power warning, port 16/9	
Condition: On enabling optical monitoring on 20x10G Line card module with SFPP optic.	
Workaround: Disable optical monitoring for the port on which the errors are seen	

Defect ID: DEFECT000553175	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.4.00	**Technology:** MPLS Traffic Engineering
Symptom: FRR may take longer than the standard 50 ms.	
Condition: Issue can be seen if any of the following conditions are true - - PIM interface and MPLS uplinks are on same physical interface. - MPLS uplink ports are using different Network Processors on LP - LDP signaling	
Workaround: - Multicast and MPLS uplinks on different physical interfaces - MPLS uplinks on same Network Processor on a single LP - MR2 Management Module instead of MR - VLL (RSVP signaled) instead of VPLS	

Defect ID: DEFECT000553391	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast Routing
Symptom: When OSPF NSR is configured and OSPF is enabled on IPsec tunnels and switchover is performed then some traffic loss may be observed during the switchover interval.	
Condition: OSPF is configured on IPsec and OSPF NSR is enabled and switchover is performed.	

Defect ID: DEFECT000554273	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: Sometimes while powering-up a chassis or any individual 8x10G LP, it can go down with the reason code "CARD_DOWN_REASON_TM_LBG_TEST_FAIL".	
Condition: This issue can be encountered while full system reload or any individual 8x10G LP reboot.	
Recovery: Power-cycling the 8x10G LP, individually, resolves the issue.	

Defect ID: DEFECT000556063	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** Syslog
Symptom: "A:PRAM free: slot 1 XPP 1 0x0007ff83 0x00000001" type messages logged during time of high ITC Queue usage .	
Condition: During a time of High ITC Queue Usage.	

Defect ID: DEFECT000556641	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: "snTrapPortConfigChange" SNMP trap may be seen for a port which doesn't change status.	
Condition: "snTrapPortConfigChange" port config change trap is seen twice after disabling a port, which is already disabled.	

Defect ID: DEFECT000559032	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: MAC table could get out of sync between the MCT chassis, cause incorrect flooding in the network in a L2 MCT configuration, when ICL link is flapped without keepalive VLAN.	
Condition: May happen when ICL flaps without keepalive VLAN in a scaled topology. Example of one such scale topology includes 4K MCT VLANs, 140 K MAC entries, 22 K ARP entries, with 200 MCT clients.	
Recovery: Clear MAC on the MCT chassis to repopulate the MAC table	

Defect ID: DEFECT000559413	**Technical Severity:** Medium
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:** IP Addressing
Symptom: Unexpected reload while updating ACL clauses.	
Condition: Updating ACL clauses associated with multicast filter applied on VE.	

Defect ID: DEFECT000559621	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: IPSec module may undergo continuous Rolling reboot due to BIST failure.	
Condition: FPGA installation could be incorrect.	

Defect ID: DEFECT000560563	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: 0.1% frame loss may be observed at line rate due to EGQ reassembly errors in case of 2X100g line cards.	
Condition: This happens only with full mesh topology. Port to port line rate traffic is not affected and no packet loss is seen.	

Defect ID: DEFECT000561541	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** xSTP - Spanning Tree Protocols
Symptom: Traffic loss may be seen for longer duration during RSTP reconvergence when link between core node routers is flapped.	
Condition: Only when multicast snooping is enabled along with RSTP on a scaled RSTP topology. Trigger for the issue is port flapping or port interface down between two core nodes where one of the nodes is RSTP root bridge.	
Workaround: 1) Configure root port as a multi-slot lag between the core nodes where one of the node is the root node. This will ensure that these are no easy link flaps. 2) Disable Multicast snooping.	

Defect ID: DEFECT000561652	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: MAC resource leak in software may be seen rarely. The available free MAC entries in software may decrease faster than in hardware.	
Condition: Rarely occurs only with MCT VPLS configuration in CES/CER.	

Defect ID: DEFECT000562162	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** LAG - Link Aggregation Group
Symptom: While changing primary and disable/enable LAG ports, observed "Error - vlandata_get_vport, next_free_vport_index 68166161" in console logs	
Condition: While changing primary and disable/enable LAG ports.	

Defect ID: DEFECT000562959	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Debug messages starting with [PRAM_FREE] may be seen on line card console.	
Condition: Only in algorithmic mode (X2 scale) during hitless upgrade operation.	

Defect ID: DEFECT000563189	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: Displaying BGP neighbor output may sometime show the error: "Duplicate session added". There is no functionality loss or impact.	
Condition: Performing MP switch-over multiple times.	

Defect ID: DEFECT000563192	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: A Syslog -- "duplicate IP address on an interface" is observed.	
Condition: Issue will be observed when either a duplicate IP address is configured or a loop is present in the network.	
Recovery: Remove the duplicate IP address configured or break the loop in the network.	

Defect ID: DEFECT000563516	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** BFD - BiDirectional Forwarding Detection
Symptom: ISIS neighbor flaps leading to traffic loss may be seen rarely.	
Condition: When unconfiguring/configuring ISIS protocol, BFD session may flap shortly after ISIS is configured.	

Defect ID: DEFECT000563805	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.7.00	**Technology:** IPv4 Multicast VLAN Traffic Reduction
Symptom: Under rare condition, if FID exhaustion occurs, some of the flows may experience traffic loss.	
Condition: UPNP (Universal Plug and Play) protocol may pump at a high rate Multicast control packets resulting in this problem.	
Workaround: Block the UPNP requests using Multicast filters.	

Defect ID: DEFECT000563946	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.6.00	**Technology:** IPv4 Multicast VLAN Traffic Reduction
Symptom: Multicast traffic impacted when VPLS snooping is enabled.	
Condition: - Seen on CER - Continuous joins and leaves and - VPLS snooping	

Defect ID: DEFECT000564005	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: With scaled ACL configuration snmpwalk on policy based accounting table may take longer than expected.	
Condition: May occur only when a duplicate (scaled) ACL configuration is applied and SNMP walk is issued while the ACL configuration update is still in process.	
Workaround: Avoid issuing snmpwalk command during ACL configuration update	

Defect ID: DEFECT000564058	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.9.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: CCEP flapping with high LP CPU may be seen, when a 24x10G card is reset using CLI command, with multi-slot CCEP LAG configuration in Dual-MCT setup.	
Condition: In Dual MCT setup with multi-slot CCEP LAG configured on 24x10G cards	

Defect ID: DEFECT000564316	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Ping may fail on a 10Gx24 line card when an OpenFlow hybrid port is configured on an unprotected VLAN.	
Condition: Hybrid OpenFlow and VE interface configured on an unprotected VLAN. The unprotected VLAN PASS entries are not created on OpenFlow ACL cam.	
Workaround: Change the configuration from an unprotected VLAN to a protected VLAN on those ports	

Defect ID: DEFECT000564805	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.9.00	**Technology:** Rate Limiting and Shaping
Symptom: Traffic loss may occur on a 100Gx2 line card when configuring the inbound port base rate limit.	
Condition: Only if configuring inbound rate limit on a 100Gx2 line card.	
Recovery: Use another type of line card.	

Defect ID: DEFECT000564808	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: High LP CPU usage may be seen due to routing table download.	
Condition: When importing more routes to a VRF via inter-vrf leaking, causing the receiving VRF's route table to run out of space.	
Workaround: Use route-map to limit the number of routes imported to a VRF in the inter-vrf leaking configuration.	
Recovery: Clear ip route table for the VRF.	

Defect ID: DEFECT000564830	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPSec Tunnel status may be down on the Management Module.	
Condition: When the tunnel outgoing port changes from one Line Card to another Line Card.	
Workaround: Avoid changing of tunnel outgoing port to another Line Card.	
Recovery: Clear or reset the affected tunnel.	

Defect ID: DEFECT000564957	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** Static Routing (IPv6)
Symptom: MP might reload unexpectedly on issuing the command "itc show queue 11".	
Condition: In a topology with the following characteristics: --- IP Sec tunnels in default VRF and underlying interface is using non-default VRF. --- There are 121 IPSec tunnels configured between two routers --- There are 100 ipv6 IPSec tunnels between two routers. If syslog reports for low buffers, then issuing command "itc show queue 11" might cause MP reload.	

Defect ID: DEFECT000565223	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: "ERROR: command not supported for this type of card" may be seen when downgrading from 5.9.00 to 5.6.00f. There is no impact to functionality.	
Condition: Downgrade system software from 5.9.00 to 5.6.00f.	

Defect ID: DEFECT000565395	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: When a BGP router sends a withdraw update message for a set of routes, the peer BGP router receiving this withdrawn message will not clear these routes; instead peer will marks them as dampened routes and will clear them after 180 minutes.	
Condition: BGP routes are not getting cleared as they are getting withdrawn.	
Workaround: The dampened routes are not included in best route calculation and will not be advertised. "clear ip bgp dampening" can be used to clear the dampened routes.	

Defect ID: DEFECT000565409	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: IPSec tunnels may stay in down state after the Line card is reloaded.	
Condition: Reload the Line card module of a remote IPSec peer.	
Recovery: Clear or reset the affected IPSec tunnels.	

Defect ID: DEFECT000565437	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.9.00	**Technology:** IPsec - IP Security
Symptom: Traffic for one of the IPv6 prefix may be sent out on the wrong IPSec tunnel if that prefix is reachable through a static route and is learnt via IGP as well.	
Condition: In IPv6 IPsec double encryption configuration; IPv6 prefix reachable through static route and learnt via IGP	

Defect ID: DEFECT000565487	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.9.00	**Technology:** MPLS Traffic Engineering
Symptom: Unexpected system reload may be seen when slot was removed in highly scaled MPLS network.	
Condition: Only if multiple protocols are scaled including MPLS and in a rare timing window.	

Defect ID: DEFECT000565571	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** IP Multicast
Reported In Release: NI 05.9.00	**Technology:** IPv4 Multicast Routing
Symptom: Loss of traffic may be seen on specific VRF post reload of the device.	
Condition: In scaled set-up when reload is performed.	
Recovery: Clear the multicast entries using "clear ip pim mc" command.	

Defect ID: DEFECT000565843	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: Salt value associated with the IPSec encryption key may be displayed as zero.	
Condition: May be seen when AES-GCM-128 algorithm is used for encryption/decryption of packets over IPSec tunnel.	

Defect ID: DEFECT000566036	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** Configuration Fundamentals
Symptom: 20x10G and 8x10G OIR (Online Insertion/Removal) may make TM CPU Queue stuck forever causing VPLS MAC learning to break.	
Condition: When MPLS L3VPN, 6VPE, VPLS traffic running on 20x10G and 8x10G modules and LP OIR is performed for either of these modules, the TM CPU Queue may get stuck.	
Recovery: To find out stuck queue: MP#show tm non-empty-queue To recover, the stuck TM CPU queue needs to be flushed once as instructed below: LP#dm tm auto-credit <device-id> 1000 <queue-id> <queue-id> After a minute: LP#dm tm auto-credit <device-id> 0 <queue-id> <queue-id>	

Defect ID: DEFECT000566210	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.9.00	**Technology:** IP Addressing
Symptom: The router restarts sometime.	
Condition: Simultaneous flapping of multiple interfaces manually through a script.	

Defect ID: DEFECT000566355	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.9.00	**Technology:** OpenFlow
Symptom: MLX device resets very rarely upon addition/removal of large number of OpenFlow flows	
Condition: Continuous Flow addition/removal for a large period of time(3-4 days)	
Workaround: Issue is not seen in 6.0 release	
Recovery: Issue is not seen in 6.0 release	

Defect ID: DEFECT000566513	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.6.00	**Technology:** MPLS VLL - Virtual Leased Line
Symptom: The System may reload while performing Switchover.	
Condition: 1. MPLS traffic should be running. 2. Switchover is done.	

Defect ID: DEFECT000567517	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** SSH - Secure Shell
Symptom: Device may unexpectedly reload when a SSH client is attempting to login to it.	
Condition: Continuous attempts (more than 200 times) to login with bad username/password using SSH.	
Workaround: User may block the source that is attempting to login with bad credentials.	

Defect ID: DEFECT000569860	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.8.00	**Technology:** OpenStack Integration
Symptom: Auto-negotiation not complete syslog is generated twice in a specific auto-negotiation configurations with MACsec enabled; only one syslog is expected.	
Condition: MACsec is enabled on the port. Auto-negotiation is disabled state at both local and remote devices. Enable auto-negotiation at local-device.	

Defect ID: DEFECT000570731	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.8.00	**Technology:** LAG - Link Aggregation Group
Symptom: On 20x10G Line card module high CPU condition could be seen when the command "no route-only" is enabled.	
Condition: "no route-only" option is enabled when there is a LAG spanning across multiple ports on the same 20 x 10G Line card module.	

Defect ID: DEFECT000571753	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** CLI - Command Line Interface
Symptom: CLI returns the error "Invalid Input" when an IP/IPv6 ACL deny filter is being configured in the IP/IPv6 ACL configuration mode.	
Condition: The issue is seen when a decimal is used that is equal in value to that of any of the valid Keywords. For ex: Keyword "tcp" is associated with a value of 6. If the same number is inputted in the command line as deny 6 a.b.c.d a.b.c.e eq 50120 log The error is seen since the optional keyword "eq" is not available in "<decimal>" node. Note: Although an error message is displayed, the command will get stored in the configuration using the associated keyword matching with number. In this case it would get stored as deny tcp a.b.c.d a.b.c.e eq 50120 log.	
Workaround: Use appropriate keyword for the deny filters instead of its decimal equivalent.	

Defect ID: DEFECT000572448	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: customers may observe message similar to the one given below on active Management Module during switchover: VRRP4: eth 1/1 down event received	
Condition: (1) VRRP is configured (2) Switchover is initiated	

Defect ID: DEFECT000572825	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: In a MCT setup : - 1) Traffic loss after switchover 2) Missing "deploy" keyword/configuration in "show cluster configuration" on the MCT cluster node on which Management module switchover was done.	
Condition: Management module switchover on one of the MCT cluster nodes.	
Workaround: 1) Save startup-config by using "write memory" command 2) Issue the command "sync-standby" before Switchover	

Defect ID: DEFECT000573260	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.4.00	**Technology:** IP Addressing
Symptom: When pinging a device directly connected to the CES from a host several router hops away, the ping traffic gets stuck in a routing loop.	
Condition: On CER/CES platform, with non-major network subnets (subnets that are not /8, /16, /24 or /32) present in network with 100s of hosts directly connected to the node.	
Recovery: clear ip ospf route all	

Defect ID: DEFECT000573265	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: On ICL flap, VPLS does not come up on MCT L2VPN peer. "show mpls vpls <> " show the cluster peer state as "MCT Peering Time-out State"	
Condition: On scaled MCT L2VPN environment (around 2000 VPLS instances and 70K MACs), ICL port flap can cause some VPLS instances not to comeup	
Recovery: "clear cluster < >" CLI, clears the problem.	

Defect ID: DEFECT000573553	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.7.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Below error message will be seen when undeploying the cluster and configuring active-passive mode for cluster. "Error - Cannot change MCT mode for cluster id = 1 when cluster deployed"	
Condition: Undeploy the cluster and configure active-passive mode for cluster	

Defect ID: DEFECT000573690	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: The following messages scrolling on telnet/ssh/console session : "SAT Error: itc_scp_check_snm - itc_send_request() failed ret[8]"	
Condition: On MLX, continuous CCEP and ICL flaps on MCT L2VPN scaled environment (2000 VPLS instances with 70K MACs).	

Defect ID: DEFECT000574287	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: MACs are not relearned after the command "clear mac vpls eth <mod/port>" is issued.	
Condition: This is not applicable to NI5.9 and later releases.	
Workaround: "clear mac vpls id <>" to clear and relearn the MACs.	

Defect ID: DEFECT000575239	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.7.00	**Technology:** OpenFlow
Symptom: Router reload while adding OpenFlow flows from an OpenFlow controller.	
Condition: OpenFlow enabled and new flow-add request has both Send to controller and VLAN Push/Pop/Modify action.	

Defect ID: DEFECT000575527	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: When client-interfaces are shut, "show cluster" shows "Peer State: CCP Down (Reason for Down: Graceful upgrade in progress)". The reason displayed is wrong. There is no functional impact.	
Condition: Seen in an MCT setup when client interfaces are shutdown administratively using the "client-interfaces shutdown" command	

Defect ID: DEFECT000575926	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Unwanted debug print messages related to enabling MCT clients interfaces will be seen in console while the device is reloaded with MCT configurations in place. The messages will be seen right after bring up of the CCP session.	
Condition: The unwanted messages will be seen with MCT configurations in place and while rebooting the Node.	
Workaround: There is no work around available.	
Recovery: Unwanted messages will NOT cause any functional impact.	

Defect ID: DEFECT000576701	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: "No deploy" of MCT L2VPN cluster does not work at times	
Condition: On scaled MCT L2VPN environment, with around 2000 VPLS instances.	
Workaround: Wait for around 30 seconds after no deploy on scaled environment.	

Defect ID: DEFECT000576911	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.9.00	**Technology:** CLI - Command Line Interface
Symptom: "show tech-support l4 acl <specific name> " output from console does not show all ACL entries.	
Condition: When more than 1700 ACLs are configured on the device and console session is used to execute ""show tech-support l4 acl <specific name> " command	
Workaround: Use Telnet/SSH to execute "show tech-support l4 acl <specific name> " command	

Defect ID: DEFECT000577144	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.6.00	**Technology:** OpenStack Integration
Symptom: 8x10G-X card fails to come Up online. Shows different status messages each time after restart of module, reseat or reload of chassis	
Condition: NA	

Defect ID: DEFECT000577652	**Technical Severity:** Low
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: Cluster FSM messages are seen in log. These messages are harmless.	
Condition: Messages such as "CLUSTER FSM: Error: Received CCP event when cluster 0x00000001 is not deployed" are observed during various MCT events	

Defect ID: DEFECT000578097	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** CLI - Command Line Interface
Symptom: Closing pattern/prompt ")#" is missing from the VPLS config mode.	
Condition: Configure VPLS instance name with length greater than 128 characters and press Enter to complete the command Note: Applicable only for releases 5.7x and lower versions	
Workaround: Avoid configuring VPLS instance name with length greater than 128 characters	

Defect ID: DEFECT000578870	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.6.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: CES/CER nodes may incorrectly send back broadcast packets received from the ICL port to the newly added member port in CCEP LAG.	
Condition: Adding a new member port to a deployed CCEP LAG.	
Workaround: (1) Disable the primary port (2) Add the member port to the deployed LAG (3) Enable primary port	
Recovery: Deploy and undeploy the LAG.	

Defect ID: DEFECT000579896	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.8.00	**Technology:** ACLs - Access Control Lists
Symptom: After Management Module switch-over occurs more than once, traffic doesn't get filtered as per the applied L2 ACL based rate-limiting binding on interface. Also, L2 ACL based rate-limiting counters don't display correct values as per the traffic filtering.	
Condition: When an active management module fails over to a standby management module or when a "switchover" command is entered manually, from the second failover onwards, the ACL based rate-limiting CAM entries aren't programmed as per the actual ACL definition.	

Defect ID: DEFECT000580586	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.8.00	**Technology:** CLI - Command Line Interface
Symptom: Observing "ITC not successful" error in CLI while disabling and enabling of loop back interface.	
Condition: Disabling and enabling of loop back interface several times with in a short span of time with highly scaled VPLS/VLL instances.	

Defect ID: DEFECT000581125	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.8.00	**Technology:** LDP - Label Distribution Protocol
Symptom: In a router configured with heavy BGP routes (~100k) with aggressive BFD configuration for IGP protocol; LDP sessions may flap if the user executes clear ip bgp neighbor all.	
Condition: The condition includes a very high scale BGP configuration, BFD, and LDP; in combination with user execution of 'clear ip bgp neighbor all'	

Defect ID: DEFECT000581687	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.8.00	**Technology:** BGP/MPLS VPN
Symptom: On clearing statistics of all MPLS tunnels, High LP CPU utilization will be observed and timeout message will be displayed in the console. LP CPU utilization will return to normal after clearing all the tunnel statistics.	
Condition: When there are more than 4K MPLS LSP tunnels and 4K IP nexthops entries.	

Defect ID: DEFECT000582617	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Action list gets corrupted for already installed flows with Normal action	
Condition: After a power-off followed by power-on of Line card.	
Recovery: Remove and add the flows again.	

Defect ID: DEFECT000582982	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.6.00	**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: Active management module in MLX may reload unexpectedly and switch over to the standby management module if available. The below mentioned stack trace could be seen in the dump: - Possible Stack Trace (function call return address list) 00005008: xsyscall(pc) 00056194: bm_alloc(lr) 00055d14: bm_alloc 0005cc94: gt6446x_eth_receive_handler 0005d230: gt6446x_eth_isr 00027234: handle_interrupt 0001b69c: sysloop 000b7dfc: handler	
Condition: When huge burst of Management Module CPU bound traffic is received	

Defect ID: DEFECT000584620	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** SDN
Reported In Release: NI 05.8.00	**Technology:** OpenFlow
Symptom: Push an OpenFlow rule with action as send to controller. Reload Line card which holds the OpenFlow rule. After the line card is operational, the packets are not forwarded to controller though traffic hits the flow.	
Condition: In case of reload of line card, the Line card will be programmed with the OpenFlow rule. In case of send to controller action OpenFlow rule, the programming went wrong which caused to packets to get dropped.	

Defect ID: DEFECT000585720	**Technical Severity:** High
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: Syslog message similar to the one mentioned below may be reported : "PRAM free: slot 5 XPP20SP 0 0x0007f5b3 0x00000001" In some cases Traffic Forwarding could be impacted.	
Condition: A message is logged when any violation is reported during the PRAM monitoring which could be indicative of double free of a PRAM index or Freeing of a PRAM index which is currently in use.	

Defect ID: DEFECT000592923	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.9.00	**Technology:** sFlow
Symptom: Port based sFlow statistics don't increment as per the monitored traffic.	
Condition: Enables sFlow monitoring on interface.	

Known Issues

This section lists open software defects with Critical, High, and Medium Technical Severity as of 4/25/2016 in NI 6.0.00. This list was updated 5/26/16.

Defect ID: DEFECT000518506	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: NI 05.7.00	**Technology:** IP Addressing
Symptom: FRR Failover takes more than 70 secs to converge on bringing down the transit link. Packet drops observed when FRR 10K and 20K LSPs failover by bringing down the transit link.	
Condition: FRR failover by bringing down the transit link.	

Defect ID: DEFECT000551348	
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: While configuring BFD or changing BFD timers, the user might see unexpected values for CFM 1-DM sessions specifically on CES/CER devices.	
Condition: CES/CER User deployment where BFD and CFM 1-DM are in use.	
Recovery: The only way to recover is resetting of device.	

Defect ID: DEFECT000562915	
Technical Severity: Medium	**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: DEFECT000566837	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.2.00	**Technology:** Traffic Queueing and Scheduling
Symptom: Jitter is outside acceptable limits for voice traffic.	
Condition: Seen on Gen2 (BR-MLX-10Gx8-M or –X and BR-LMX-100Gx1-X or x2-X) Line cards with low throughput traffic.	

Defect ID: DEFECT000575538	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 05.6.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: When issuing SNMP walk for lldpRemTable, some of the LLDP neighbors object will not be displayed.	
Condition: When any of the objects under the table "lldpRemTable" are not configured.	

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: 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 the interface 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: DEFECT000579366	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Network Automation and Orchestration
Reported In Release: NI 05.8.00	**Technology:** OpenStack Integration
Symptom: PAUSE frames received on an interface are not honored even though "flow-control rx-pause-ignore" is not configured.	
Condition: When "no flow-control" is configured at interface level.	
Workaround: Apply "no flow-control rx-pause-ignore" at interface level	

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: DEFECT000580123	
Technical Severity: High	**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: 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 remote end was removed. 2. When the remote end device is Infinera WDM/DTN-X device	
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 06.0.00	**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 a few of the line cards with scaled configuration of MAC/IPv4/IPv6 ACLs.	
Condition: When user configures a scaled number of MAC/IPv4/IPv6 ACLs, Management module takes significant amount of time to complete synchronization of the configuration to all the Line cards. In rare conditions, the synchronization of configurations can fail resulting in the ACL configuration not present in the Line card.	

Defect ID: DEFECT000586070	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.9.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Mac-address seen to loop between local interface and remote interfaces towards MCT cluster.	
Condition: On CER, MCT VPLS with CoS configuration in LSP.	
Workaround: Issue will not be seen if CoS configuration is not present in LSP.	

Defect ID: DEFECT000587054	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 05.7.00	**Technology:** Hardware Monitoring
Symptom: In certain configuration, a 100G interface may not come up in an operational state.	
Condition: Due to the state of the link parameters, an interface link goes down.	
Recovery: Setting interface to disable and re-enabling it fixes the issue.	

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 the BGP operation and starts again.	

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 Line card module failing to process packets with error “RX Lookup unavailable”.	
Condition: CAM FIFOs are stuck resulting in RX Lookup failure.	
Recovery: Reload the affected Line card module.	

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: 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: DEFECT000588168	
Technical Severity: Medium	**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: DEFECT000589295	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** Software Installation & Upgrade
Symptom: The error messages "Master Dload chksum Fail" and "firmware download failed" will be seen on line card console during initialization.	
Condition: Specifically with 2x100GE-CFP2 line card with CFP2-QSFP28 adapter plugged-in.	

Defect ID: DEFECT000589304	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: The optical module type in the syslog message - "Optic module not factory qualified", shows as "******Unknown*****" at times instead of “100GE QSFP28-AOC".	
Condition: Specifically with 2x100GE-CFP2 with CFP2 adapter and 100G QSFP28 AOC plugged-in.	

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: Happens on a scaled scenario on a slow server with a response time more than 10 seconds. No path is available for the LSPs, so the LSPs keep retrying.	
Condition: We expect the server to have a good response time within milliseconds, as that is one of the main purposes of using PCE. The issue was seen only when using a Spirent 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 a 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: DEFECT000591015	
Technical Severity: High	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** MPLS
Reported In Release: NI 05.8.00	**Technology:** MPLS VPLS - Virtual Private LAN Services
Symptom: Traffic loss In MCT VPLS scenario, after Primary MCT peer reload.	
Condition: When the Primary MCT peer fails with scaled VPLS can cause the issue.	

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: DEFECT000591513	
Technical Severity: High	**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	**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: 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 an 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: DEFECT000592026	
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: MEP ages out after Standby Management Module is reloaded	
Condition: ERP is configured with sub-second CCM interval and standby Management Module is reloaded.	

Defect ID: DEFECT000592027	
Technical Severity: Medium	**Probability:** High
Product: Brocade NetIron OS	**Technology Group:** Monitoring
Reported In Release: NI 06.0.00	**Technology:** Hardware Monitoring
Symptom: Connected to Line card, Ran the Diag bist command multiple times, after few instances LP is rebooting.	
Condition: debuggability	

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 because it doesn't match the RRO it was expecting. Thus LSP won't come up.	
Condition: This issue must be one of the corner scenarios that might be existing in the RSVP code.	
Workaround: Unconfigure 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: DEFECT000593492	
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: 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: 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: DEFECT000594168	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Security
Reported In Release: NI 05.6.00	**Technology:** ACLs - Access Control Lists
Symptom: Packets matching the permit clause of IPV6 ACL are dropped	
Condition: When MAC ACL is applied on the interface and IPV6 receive ACL rate-limiting with strict-acl option is applied globally.	

Defect ID: DEFECT000594173	
Technical Severity: Medium	**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	**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 a 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.	

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 Line card 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 reset with the below syslog and stack trace without any user intervention. It is rarely seen. 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: Rarely seen. Corner case	
Workaround: No workaround	
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 doesn't have routes in routing table which are required for multicast source and RP lookup.	
Workaround: Make sure unicast routing table populated before running multicast traffic.	

Defect ID: DEFECT000595623	
Technical Severity: Medium	**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: 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 an 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: DEFECT000595703	
Technical Severity: High	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: NI 05.4.00	**Technology:** MCT - Multi-Chassis Trunking
Symptom: High LP CPU usage	
Condition: MLX-32 with MCT configuration	

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 IGP neighbor down event and no path is available.	
Condition: The system has IGP sync enabled and an LSP has selected path as the Active path and in addition to that there is no alternated path for the selected secondary to come UP. Under these conditions, if an interface flap in the network triggers 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: 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: DEFECT000596126	
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: 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	**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: 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: Contact Brocade Support for guidance on how 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 restarts sometime.	
Condition: When BFD sessions are established over LAG ports.	

Defect ID: DEFECT000596272	
Technical Severity: High	**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	**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: 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:	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. 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 happens after all this, the error code of the LSP will be incorrect.
Condition:	Happens and is 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: DEFECT000597226	
Technical Severity: High	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.9.00	**Technology:** Traffic Queueing and Scheduling
Symptom:	While upgrading to a newer version, some of the SFM may go down.
Condition:	This issue is seen rarely.
Recovery:	Power cycle the SFM that has gone down and the issue will not be seen.

Defect ID: DEFECT000597413	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade NetIron OS	**Technology Group:** Traffic Management
Reported In Release: NI 05.6.00	**Technology:** Rate Limiting and Shaping
Symptom: Link fault signaling settings is not applied after reloading the chassis.	
Condition: Link fault signaling enabled globally and then reload chassis or power cycle LP.	
Recovery: Disable and enable link-fault-signaling globally.	

Defect ID: DEFECT000597443	
Technical Severity: High	**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 came up but its 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	