April 2, 2019

NetIron OS 6.0.00j for ExtremeRouting MLX Series Devices

Release Notes v2.0

9036087-01

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial release	11 March 2019
2.0	Added defects NI-14772, NI-9881, NI-9883, NI-8795, and NI-9233 to defect section, “Closed with Code changes R06.0.00j”.	2 April 2019

Preface

Contacting Extreme Technical Support

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

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

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

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

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

Extreme resources

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

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

Document feedback

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

You can provide feedback in two ways:

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

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

Overview

NetIron OS Release 6.0.00 introduces new functionalities and enhances the capabilities of ExtremeRouting MLX Series, ExtremeRouting CER 2000 Series and ExtremeSwitching CES 2000 Series devices. Extreme 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,
- Extreme 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, MLX Series continues as the leading platform for converged data center and service provider network services.

Extreme 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 MLXe device chassis into Packet Broker mode.
- Installing the MAIN (default) FPGA bundle will place the 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 R6.0.00j.

  There are no deprecated commands in R6.0.00h.

  There are no deprecated commands in R06.0.00g.

  There are no deprecated commands in R06.0.00f.

  There are no deprecated commands in R06.0.00e.

  There are no deprecated commands in R06.0.00d.

  There are no deprecated commands in R06.0.00c.

  There are no deprecated commands in R06.0.00b.

  There are no deprecated commands in R06.0.00a.

Software Features

New software features introduced in R06.0.00j

There are no new software features introduced in R06.0.00j.

New software features introduced in R6.0.00h

Details of corrected defects are provided in Closed with Code changes R6.0.00h.

The following new features are introduced in R6.0.00h:

LLDP enhancement – LLDP feature has been enhanced to provide the option to configure the subtype for LLDP port-id which is advertised to the receiving device which displays this info as port-id-subtype info of its neighbor. The **lldp advertise port-id-subtype** command is introduced to advertise interface-alias or interface-name or mac-address as LLDP.

entaliasmapping table – This enables the polling of entAliasMappingIdentifier in entAliasMappingTable based on entphysical index to return ifIndex of interface ports.

New software features introduced in R6.0.00g

There are no new software features introduced in R6.0.00g.

Details of corrected defects are provided in Closed with Code changes R6.0.00g.

New software features introduced in R06.0.00f

Details of corrected defects are provided in Closed with Code changes R06.0.00f.

The following new feature is introduced in R06.0.00f.

Fabric link balancing – This feature supports balancing fabric links to avoid congestion when a link is brought down by software monitoring. The software will also bring down the other link pair so the fabric links are balanced.

New software features introduced in R06.0.00e

There are no new software features introduced in R06.0.00e.

New software features introduced in R06.0.00d

Details of corrected defects are provided in Closed with Code changes R06.0.00d.

Enhanced features introduced in R06.0.00d:

- **VLAN name length change** - This feature supports up to 35 characters of the VLAN name. The VLAN name character length is increased from 31 to 35 characters.
- **Scaling IPv4 Max-route per VRF** – This feature increases the capacity of IPv4 non-default VRF routes from 650K to 750K. By default, the system-max values for ip-route and ip-cache are increased from 650K to 750K to accommodate the max-route scale.

New software features introduced in R06.0.00c

Details of corrected defects are provided in Closed with Code changes R06.0.00c.

Enhanced features introduced in R06.0.00c:

- **Saving system state to Flash** - This feature aims to collect/capture system state information for debugging purposes at the customer site.
- **Longest Prefix Match Next Hop Walk** - This feature detects inconsistencies between the software and the hardware LPM next hop programming and can generate a syslog warning or take a corrective action to clear the affected routes.

New software features introduced in R06.0.00b

Details of corrected defects are provided in Closed with Code changes R06.0.00b.

Enhanced features introduced in R06.0.00b:

- **Preserving EXP bits in MPLS header** - Preserves the traffic class based on the EXP value from the MPLS header for the VPLS/VLL traffic from the MPLS uplink. Traffic is queued based on the extracted EXP/traffic class value from the packet.
- **Exclude PCP Marking** - With this ACL option, irrespective of priority-force, the packet's pcp value will not be modified on any packet L2/L3/VPLS.
- **Recovery using NP MAC FIFO reset on detecting MAC FIFO Full condition** - This feature monitors the NP Memory MAC FIFO full error condition and allows auto recovery of the system in cases of MAC FIFO full error. This feature will attempt to reset the FIFO for recovery when FIFO full condition is latched.
- **Logging hardware error from Tsec statistics and LP IPC buffer corruption into syslog/console** - This feature monitors Tsec (backplane LP Ethernet controller) for three types of the errors latched in Tsec like FCS error, code error and carrier sense error while receiving the packet from management card.
- **CRC check on Hi-Gig header in Rx path** - This feature is disabled by default. A command has been provided to enable Hi Gig CRC check on Rx path.
- **Flow Control Status** - This feature provides a consolidated view of the flow control status information, including pause frames received by the ports, at various sub-system levels of the line card.

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 R6.0.00j

There are no new CLI commands in R06.0.00j.

New CLI commands R6.0.00h

lldp advertise port-id-subtype

New CLI commands R6.0.00g

There are no new CLI commands in R06.0.00g.

New CLI commands R06.0.00f

There are no new CLI commands in R06.0.00f.

New CLI commands R06.0.00e

There are no new CLI commands in R06.0.00e.

Modified commands in R06.0.00d

The following commands have been modified in this release.

- Vlan *vlan-id* [name *vlan-name*]
- system-max ip-vrf-route *num*

Modified commands in R6.0.00h

The following commands have been modified in this release.

- show lldp local-info
- show lldp neighbor
- show lldp neighbor detail

New CLI commands R06.0.00c

- memdump slot-*slot-id*
- reload-memdump
- reset-memdump
- [no] sysmon lpm nh-walk { action *action-selection* | auto| polling-period *duration* | threshold *threshold-setting*}
- Show sysmon lpm nh-walk status
- [no] sysmon lpm nh-walk start

New CLI commands R06.0.00b

- [no] set-force-tc-match-label-exp
- [no] access-list 1200 permit any any any etype any priority-mapping priority-force exclude-pcp-marking
- show flow-ctrl *status all*

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 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

No MIB objects were introduced in release R6.0.00j.

New MIB Objects

No MIB objects were introduced in release R6.0.00h.

New MIB Objects

No MIB objects were introduced in release R6.0.00g.

New MIB Objects

No MIB objects were introduced in release R06.0.00f.

New MIB Objects

No MIB objects were introduced in release R06.0.00e.

New MIB Objects

No MIB objects were introduced in release R06.0.00d.

New MIB Objects

No MIB objects were introduced in release R06.0.00c.

New MIB Objects

No MIB objects were introduced in release R06.0.00b.

MIB Objects

The following MIB objects are introduced in release R06.0.00a:

- 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 R6.0.00j

The following devices are supported in this release:

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

Supported devices for Network Packet Broker R6.0.00j

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

Supported modules

The following interface modules are supported in this release:

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

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-100GX2-CFP2-M	MLX 2-port 100 GbE (M) CFP2 module. Supports 512,000 IPv4 routes in FIB.	Yes	Yes	3
BR-MLX-100GX2-CFP2-X2	MLX 2-port 100 GbE (X2) CFP2 module with extended route table support for up to 2.4 million IPv4 or 1.8 million IPv6 routes in hardware.	Yes	Yes	3
BR-MLX-100GX1-X	MLX Series 1-port 100 GbE module with IPv4/IPv6/MPLS hardware support—requires high-speed switch fabric modules and CFP optics.	Yes	Yes	2
BR-MLX-100GX2-X	MLX Series 2-port 100 GbE module with IPv4/IPv6/MPLS hardware support—requires high-speed switch fabric modules and CFP optics.	Yes	Yes	2
BR-MLX-10GX8-X	MLX Series 8-port 10 GbE (X) module with IPv4/IPv6/MPLS hardware support—requires SFP optics. Supports up to 1 million IPv4 routes in FIB. Requires high-speed switch fabric modules.	Yes	Yes	2
BR-MLX-1GCX24-X	MLX 24-port (X) 10/100/1,000 copper (RJ-45) module with IPv4/IPv6/MPLS hardware support. Supports 1 million IPv4 routes in hardware.	Yes	Yes	1.1

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

Module	Description	Compatible devices		Generation
		MLXe with MLX or MR2-M mgmt. module	MLXe with XMR or MR2-X mgmt. module	
BR-MLX-1GFX24-X	MLX Series 24-port FE/GbE (SFP) module, with IPv4/IPv6/MPLS hardware support. Supports 1 million IPv4 routes in hardware.	Yes	Yes	1.1
BR-MLX-1GFX24-X-ML	MLX Series 24-port FE/GbE (SFP) module, with IPv4/IPv6/MPLS hardware support. Supports 512,000 IPv4 routes in FIB. License upgradable to "X" scalability (1 million IPv4 routes in hardware).	Yes	No	1.1
BR-MLX-10GX24-DM	MLXe 24-port 10 GbE module with IPv4/IPv6/MPLS hardware support—requires SFP optics. Supports 256,000 IPv4 routes in FIB.	Yes	No	3a
NI-MLX-1GX48-T-A	MLX Series 48-port 10/100/1000BASE-T, MRJ21 module with IPv4/IPv6/MPLS hardware support.	Yes	No	1.1
NI-MLX-10GX8-D	MLX Series 8-port 10-GbE (D) module with IPv4/IPv6 hardware support - requires SFPP optics. Supports 256K IPv4 routes in FIB. Does not support MPLS. Requires high speed switch fabric modules.	Yes	No	2

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

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

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

Supported power supplies

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

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

Supported optics

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

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.extremenetworks.com. In some cases, boot and manifest images do not need to be upgraded.

MLX Series and XMR Series devices

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

Required images for R6.0.00j MLX Series/XMR Series software upgrade

Manifest File for XMR/MLX Release 06.0.00

-NETIRON_IRONWARE_VER XMR-MLXV6.0.00j
#==
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin
-DIRECTORY /Boot/ManagementModule
xmprm05900.bin
Application Images
-DIRECTORY /Combined/FPGA
lpfpga06000j.bin
-DIRECTORY /Combined/Application
xm06000j.bin
-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin
-DIRECTORY /Monitor/ManagementModule
xmb06000.bin
-DIRECTORY /Application/ManagementModule
xmr06000j.bin
-DIRECTORY /Application/InterfaceModule
xmlp06000j.bin
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06000j.bin 2.05
pbif8x10_06000j.bin 2.24
pbifmrj_06000j.bin 4.04
pbifsp2_06000j.bin 4.02
statsmrj_06000j.bin 0.09
xgmacsp2_06000j.bin 0.17
xpp2x100_06000j.bin 1.05
xpp4x40_06000j.bin 6.00
xpp4x10g3_06000j.bin 5.00
xpp8x10_06000j.bin 1.08
xppmrj_06000j.bin 1.03

xppsp2_06000j.bin 1.01
xppxsp2_06000j.bin 1.01
pbif-ber-g3_06000j.bin 2.05
xpp20x10g3_06000j.bin 6.04
xpp2x100g3_06000j.bin 6.04
-DIRECTORY /FPGA/ManagementModule
mbridge32_06000j.xsvf 36
mbridge_06000j.xsvf 37
sbridge_06000j.mcs 6
hsbridge_06000j.mcs 17
-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06000.sig
xmb06000.sig
xmr06000j.sig
xmlp06000j.sig
lpfpga06000j.sig
hsbridge_06000j.sig
mbridge_06000j.sig
mbridge32_06000j.sig
sbridge_06000j.sig
pbif4x40_06000j.sig
pbif8x10_06000j.sig
pbifmrj_06000j.sig
pbifsp2_06000j.sig
pbif-ber-g3_06000j.sig
statsmrj_06000j.sig
xgmacsp2_06000j.sig
xpp2x100_06000j.sig
xpp20x10g3_06000j.sig
xpp2x100g3_06000j.sig
xpp4x40_06000j.sig
xpp4x10g3_06000j.sig
xpp8x10_06000j.sig
xppmrj_06000j.sig
xppsp2_06000j.sig
xppxsp2_06000j.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
xmr06000j.sha256
xmlp06000j.sha256
lpfpga06000j.sha256
hsbridge_06000j.sha256

mbridge_06000j.sha256
mbridge32_06000j.sha256
sbridge_06000j.sha256
pbif4x40_06000j.sha256
pbif8x10_06000j.sha256
pbifmrj_06000j.sha256
pbifsp2_06000j.sha256
pbif-ber-g3_06000j.sha256
statsmrj_06000j.sha256
xgmacsp2_06000j.sha256
xpp2x100_06000j.sha256
xpp20x10g3_06000j.sha256
xpp2x100g3_06000j.sha256
xpp4x40_06000j.sha256
xpp4x10g3_06000j.sha256
xpp8x10_06000j.sha256
xppmrj_06000j.sha256
xppsp2_06000j.sha256
xppxsp2_06000j.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
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

CES 2000 Series and CER 2000 Series devices

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

Required images for R6.0.00j software upgrade

-NETIRON_IRONWARE_VER CES-CERV6.0.00j
#==========
-DIRECTORY /Boot
ceb06000.bin
-DIRECTORY /Application
ce06000j.bin
-DIRECTORY /FPGA
pbifmetro_06000j.bin
-END_OF_IMAGES

-DIRECTORY /Signatures
ceb06000.sig
ce06000j.sig
pbifmetro_06000j.sig
ceb06000.sha256
ce06000j.sha256
pbifmetro_06000j.sha256
-DIRECTORY /MIBS
ce06000j.mib
ce06000j_std.mib

Manifest for Network Packet Broker devices

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

Required images for Network Packet Broker R6.0.00j software upgrade

-NETIRON_IRONWARE_VER XMR-MLXV6.0.00j
#==========
-DIRECTORY /Boot/InterfaceModule
xmlprm05900.bin
-DIRECTORY /Boot/ManagementModule
xmprm05900.bin
Application Images
-DIRECTORY /Combined/FPGA
lpfpga_npb_06000j.bin
-DIRECTORY /Combined/Application
xm06000j.bin
-DIRECTORY /Monitor/InterfaceModule
xmlb06000.bin
-DIRECTORY /Monitor/ManagementModule
xmb06000.bin
-DIRECTORY /Application/ManagementModule
xmr06000j.bin
-DIRECTORY /Application/InterfaceModule
xmlp06000j.bin
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_06000j.bin 2.05
pbif8x10_06000j.bin 2.24
pbifmrj_06000j.bin 4.04
pbifsp2_06000j.bin 4.02
statsmrj_06000j.bin 0.09
xgmacsp2_06000j.bin 0.17
xpp2x100_06000j.bin 1.05
xpp4x40_06000j.bin 6.00
xpp4x10g3_06000j.bin 5.00
xpp8x10_06000j.bin 1.08
xppmrj_06000j.bin 1.03
xppsp2_06000j.bin 1.01
xppxsp2_06000j.bin 1.01
pbif-ber-g3_06000j.bin 2.05
xpp20x10g3_npb_06000j.bin 6.14
xpp2x100g3_npb_06000j.bin 6.14
-DIRECTORY /FPGA/ManagementModule
mbridge32_06000j.xsvf 36
mbridge_06000j.xsvf 37
sbridge_06000j.mcs 6
hsbridge_06000j.mcs 17

-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05900.sig
xmprm05900.sig
xmlb06000.sig
xmb06000.sig
xmr06000j.sig
xmlp06000j.sig
lpfpga_npb_06000j.sig
hsbridge_06000j.sig
mbridge_06000j.sig
mbridge32_06000j.sig
sbridge_06000j.sig
pbif4x40_06000j.sig
pbif8x10_06000j.sig
pbifmrj_06000j.sig
pbifsp2_06000j.sig
pbif-ber-g3_06000j.sig
statsmrj_06000j.sig
xgmacsp2_06000j.sig
xpp2x100_06000j.sig
xpp20x10g3_npb_06000j.sig
xpp2x100g3_npb_06000j.sig
xpp4x40_06000j.sig
xpp4x10g3_06000j.sig
xpp8x10_06000j.sig
xppmrj_06000j.sig
xppsp2_06000j.sig
xppxsp2_06000j.sig
xmlprm05900.sha256
xmprm05900.sha256
xmlb06000.sha256
xmb06000.sha256
xmr06000j.sha256
xmlp06000j.sha256
lpfpga_npb_06000j.sha256
hsbridge_06000j.sha256
mbridge_06000j.sha256
mbridge32_06000j.sha256
sbridge_06000j.sha256
pbif4x40_06000j.sha256
pbif8x10_06000j.sha256
pbifmrj_06000j.sha256
pbifsp2_06000j.sha256
pbif-ber-g3_06000j.sha256
statsmrj_06000j.sha256
xgmacsp2_06000j.sha256

xpp2x100_06000j.sha256
xpp20x10g3_npb_06000j.sha256
xpp2x100g3_npb_06000j.sha256
xpp4x40_06000j.sha256
xpp4x10g3_06000j.sha256
xpp8x10_06000j.sha256
xppmrj_06000j.sha256
xppsp2_06000j.sha256
xppxsp2_06000j.sha256
MIBS:
-DIRECTORY /MIBS
xmr06000j.mib
xmr06000j_std.mib

Migration path

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

Upgrade and downgrade considerations

To upgrade to 6.0.00a, a two-step approach may be required.

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 = 4.02, Build Time = 8/26/2013 14:30:00

Valid XPP Version = 1.01, Build Time = 9/6/2013 14:17:00



XGMAC-2 0
XGMAC-2 1
666 MHz MPC MPC8541E (version 8020/0020) 333 MHz bus
512 KB Boot Flash (MX29LV040C), 16 MB Code Flash (MT28F640J3)
512 MB DRAM, 8 KB SRAM

...
...

Boot     : Version 5.9.0T175 Copyright (c) 2017-2018 Extreme Networks, 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) 2017-2018 Extreme Networks, INC.
Compiled on Apr 28 2016 at 02:42:58 labeled as xmlb05900b1
 (571381 bytes) from code flash
IronWare : Version 5.9.0T177 Copyright (c) 2017-2018 Extreme Networks, INC.
Compiled on Apr 23 2018 at 04:02:04 labeled as xmlp05900b1
 (9558947 bytes) from Primary
FPGA versions:
```

```
Valid PBIF Version = 4.04, Build Time = 11/10/2014 22:10:00

Valid XPP Version = 1.03, Build Time = 6/30/2016 10:37:00


...
...
...

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.

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

Hitless upgrade support

Hitless Upgrade is supported from R6.0.00g and R6.0.00h to R6.0.00j.

Limitations and restrictions

Scalability

All scalability limits are subject to change. The limits noted in this section apply to all the platforms listed unless otherwise specified.

Scalability limits	MLX Series
IPv4 non-default VRF routes	750K
System max ip-route and ip-cache	750K
Address family IPv4 max-route	750K

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

CES device (512M memory) recommendations.

- CES device 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.
- CES device 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.
- CES device 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-1GCx24-X 24-port 10/100/1000Base-T Copper Module (Serial #:
BNA0427K002, Part #: 60-1001878-11)
License: MLX-1Gx24-X-Upgrade (LID: dpcFJHMmFFH)
Boot     : Version 5.9.0T175 Copyright (c) 2017-2018 Extreme Networks, 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) 2017-2018 Extreme Networks, INC.
Compiled on Apr 28 2016 at 02:42:58 labeled as xmlb05900b1
(571381 bytes) from code flash
IronWare : Version 5.9.0T177 Copyright (c) 2017-2018 Extreme Networks, INC.
Compiled on Apr 23 2018 at 04:02:04 labeled as xmlp05900b1
(9558947 bytes) from Primary
FPGA versions:
Valid PBIF Version = 4.04, Build Time = 11/10/2014 22:10:00

Valid XPP Version = 1.03, Build Time = 6/30/2016 10:37:00

BCM56512GMAC 0
BCM56512GMAC 1
666 MHz MPC MPC8541E (version 8020/0020) 333 MHz bus
512 KB Boot Flash (MX29LV040C), 16 MB Code Flash (MT28F128J3)
1024 MB DRAM, 8 KB SRAM
LP Slot 4 uptime is 22 minutes 5 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 https://extremeportal.force.com/ (note that TSBs are generated for all Extreme platforms and products, so not all TSBs apply to this release).

TSB issues resolved in 6.0c

TSB	Summary
TSB 2016-249-A	On a NetIron device running NetIron 05.8.00 and later releases up to and including 06.1.00, the management module may unexpectedly reload when a scanning tool is accessing the NetIron device to scan SSH port 22 continuously, corrupting the data structure of an existing SSH session. This may result in an unexpected reload.
TSB 2016-248-A	On a NetIron XMR/MLX device running NI 05.8.00 or later versions up to 06.1.00, GRE and IPv6-over-IPv4 traffic transiting through a non-default VRF will be dropped if "tunnel-mode" is configured.

TSB issues resolved in 6.0ab

TSB	Summary
TSB 2016-242-A	For a critical defect (DEFECT 617836) causing unexpected MLX Line Card reloads. Brocade strongly recommends that all customers running the affected releases upgrade to releases with the fix, whether IPSec is configured or not.

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 R6.0.00j

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 03/05/2019 in NI 6.0.00j.

Note: NetIron OS R6.0.00g and R6.0.00h are not available from the Extreme Portal. Refer to NetIron OS R6.0.00j for the latest code updates. For more information, please contact Extreme GTAC Support - www.extremenetworks.com/support/contact.

Defect ID:	NI-17675		
Technical Severity:	S2 - High	**Probability:**	Medium
Product:	Extreme NetIron OS	**Technology:**	Layer 2 Technology
Reported in Release:	NI 06.0.00g	**Technology Area:**	LACP
Symptom:	LACP ports stuck in blocked state and stopped forwarding traffic. Failure to program the Topo Table is not limited to the 8x10G module. Following error messages may be observed in sysmon log, Rx Dispatch Control Path Parity Error on port range x/y – x/z Topo Table Read Packet Parity Error on port range x/y – x/z		
Condition:	1. It is observed on 8x10G after upgrade from 6.0g or 6.0h 2. LACP links configured with Per VLAN (r) STP on an untagged port		
Workaround:	Physically move links to port supported by the other TM in the affected card; Eg. On an 8x10G card if the issue is on port 5-8, relocate to any port 1-4. • TM Range verification can be done with command “show tm statistics”		

Defect ID:	NI-14772		
Technical Severity:	High	**Probability:**	High
Product:	Extreme NetIron OS	**Technology:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00gd	**Technology Area:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Router LSA links may stuck in STUB type with OSPF neighbors in FULL or LOADING state.		
Condition:	1. The OSPF ABR upgraded to 6.0gd 2. ABR has at least 3 neighbors including 1 or 2 in non-backbone areas and originates more than 2000 Summary LSAs		
Recovery:	Clear ip ospf neighbor <neighbor ip address>		

Defect ID:	NI-9881		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme NetIron OS	**Technology:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00	**Technology Area:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF retransmit queue may get stuck. This can be observed from 'show ip ospf neighbor' cnt value.		
Condition:	1. Redistribution of other protocol (or static) routes into OSPF 2. A network event that causes a flap in Forwarding Address reachability (that is, it becomes unreachable and comes back within minimum LSA interval)		
Workaround:	Clear ip route <route redistributed to OSPF>		

Defect ID:	NI-9883		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme NetIron OS	**Technology:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00	**Technology Area:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF may not withdraw routes that are redistributed from BGP.		
Condition:	1. OSPF & BGP forms Neighborship/Peering on the same interface 2. BGP advertises 8k routes or more, that are redistributed into OSPF 3. BGP session goes down		

Defect ID:	NI-8795		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme NetIron OS	**Technology:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.1.00	**Technology Area:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Customer may observe corrupted Netmask in Summary LSA		
Condition:	1. Overlapping multiple intra area prefix which will be originated as summary on ABR. 2. Withdrawal of any overlapped prefix.		

Defect ID:	NI-9233		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme NetIron OS	**Technology:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00	**Technology Area:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Routes may not get exchanged between OSPF neighbors.		
Condition:	Self-originated LSA refresh, when retransmit count is exceeded.		
Recovery:	Clear ip ospf route <Link ID>		

Closed with code changes R6.0.00h

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 01/14/2018 in NI 6.0.00h.

Issue ID:	NI-10498		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 05.8.00f	**Technology:**	NTP - Network Time Protocol
Symptom:	MLX, CES/CER may display incorrect Daylight/Summer time.		
Condition:	For Australia (GMT+10) and New Zealand (GMT+12) time zones.		

Issue ID:	NI-10512		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 05.8.00fb	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	The maximum response time for SNMP polling may go around 300msec.		
Condition:	SNMP walk for snIfOpticalMonitoringInfoTable.		

Issue ID:	NI-10522		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	MPLS
Reported in Release:	NI 05.8.00h	**Technology:**	IPv6 over MPLS VPN
Symptom:	IPv6 ping over VRF for remote BGP prefixes may not work on loopback interfaces.		
Condition:	IPv6 prefixes learnt on user-VRF loopback interface through BGP over MPLS.		

Issue ID:	NI-10814		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	MPLS
Reported in Release:	NI 06.0.00a	**Technology:**	MPLS Traffic Engineering
Symptom:	Device may reload unexpectedly with the following stack trace:- Possible Stack Trace (function call return address list) 2159f290: rrr_pkt_edit_recv(pc) 2159f260: rrr_pkt_edit_recv(lr) 21d1adf8: rsvp_pkt_process 21d19b48: rrr_rcv_rsvp_message 21d8da74: rrr_rcv_sck_data_msg2 21d8d7a8: rrr_rcv_sck_data_msg 21d8a970: rrip_sock_to_rsvp_proc 21dae0ac: rri_receive_proc 214a1a7c: nbb_dispatch_process 214a0eb8: nbb_schedule_one 214a1370: nbb_scheduler 214af9d4: nbb_spin_start 214a49d8: nbs_spin_start 216aef54: mpls_rsvp_recive_data_itc_callback 20b8fe8c: itc_process_msgs_internal 20b90338: itc_process_msgs 2170a434: mpls_task 00005e18: sys_end_task		
Condition:	On reception of Malformed MPLS RSVP Hello packet.		
Workaround:	Disable RSVP Hello Packet from the peer		

Issue ID:	NI-10860		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	MPLS
Reported in Release:	NI 06.0.00d	**Technology:**	MPLS Traffic Engineering
Symptom:	FRR Facility backup LSP is not up.		
Condition:	When "ip ospf passive" is configured on interface, there is no notification sent to MPLS deamon to cause TE flush or RSVP IGP sync reaction.		

Issue ID:	NI-10907		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.0.00f	**Technology:**	ACLs - Access Control Lists
Symptom:	The command 'ipv6 receive deactivate-acl-all' may not work sometimes.		
Condition:	Observed after router reload.		

Issue ID:	NI-10915		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP static network routes might not get advertised to the peers.		
Condition:	On Reload with BGP "static-network" routes configured. Note: This may be observed from NI6.0 and higher releases only.		

Issue ID:	NI-10961		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	NI 06.2.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	Link may stay Up even though it is disabled in CLI.		
Condition:	"loop back system" configured on the disabled port.		
Workaround:	Loop back system should be configured on enabled port.		

Issue ID:	NI-11760		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	NI 05.8.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	"show lacp" command output may display max 64bit value initially.		
Condition:	Unless a corresponding LACP packet is actually received or sent.		

Issue ID:	NI-12442		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 05.8.00c	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP task may cause High CPU.		
Condition:	Polling the OIDs of the tables .ipNetToPhysicalTable.(1.3.6.1.2.1.4.35) and .ipNetToMediaTable.(1.3.6.1.2.1.4.22).		

Issue ID:	NI-12910		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported in Release:	NI 05.8.00bn	**Technology:**	sFlow
Symptom:	Extended MPLS VC data and Switch data's outgoing 802.1q VLAN may not be observed in SFLOW forwarded packets.		
Condition:	SFLOW enabled for VPLS local switched packets.		

Issue ID:	NI-13488		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 05.9.00ba	**Technology:**	CLI - Command Line Interface
Symptom:	'Show media' and 'show optic' may display "N/A" or "NOT SUPPORTED".		
Condition:	Line card reloaded with 'loopback system' configured on port/interface.		

Issue ID:	NI-13599		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 05.8.00ec	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Standby Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 20ec94d4: bgp_check_for_fwd_address(pc) 20ec93ec: bgp_check_for_fwd_address(lr) 20efbd18: bgp_RIB_in_delete_route 20f7952c: bgp_check_for_aggrgation 20effd40: bgp_remove_route_advertisement 20efbdf4: bgp_RIB_in_delete_route 20efda08: bgp_vrf_RIB_in_delete_all_self_nlris 20eb4e88: bgp_clear_all_vrf_neighbors 20f57744: bgp_clear_neighbor_itc_request_callback 20b14584: itc_process_msgs_internal 20b14a24: itc_process_msgs 20f73ed8: bgp_task 00005e18: sys_end_task		
Condition:	Execution of "clear ip bgp neighbor all" command.		

Issue ID:	NI-13759		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.1.00	**Technology:**	IPsec - IP Security
Symptom:	IPsec tunnel session would not come up.		
Condition:	This could happen when the IPsec configuration on a linecard module is out of sync with the management module.		

Issue ID:	NI-13928		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00b	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Static routes may not be advertised into BGP.		
Condition:	1. BGP neighborship is established with the neighbor 2. "filter-change-update-delay 0" is configured 3. Static routes are configured and redistributed into BGP 4. Reload the chassis		

Issue ID:	NI-14055		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 05.8.00g	**Technology:**	Static Routing (IPv4)
Symptom:	CPU may go High with the following ITC Queue full messages:- dest app id = 0x0000000c : src app id = 0x00000014 : msg type = 0x00140002 : error = ITC_ERR_DEST_QUEUE_FULL.		
Condition:	12k IPv4 or IPv6 static routes.		

Issue ID:	NI-14078		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	MPLS
Reported in Release:	NI 05.8.00fb	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	Line card may reload unexpectedly with the following stack trace:- Possible Stack Trace (function call return address list) 20f75174: traverse_all_ports_for_local_interface(pc) 20f75084: traverse_all_ports_for_local_interface(lr) 20df9abc: lp_vpls_dy_sync_tlv_port_config 20df7050: lp_vpls_dy_sync_tlv_process_dy_messages 20bb6718: process_dy_change_packet 20bfba30: ipc_multi_module_handler 20bfdcf0: ipc_process_messages 20bfe4b0: ipc_receive_packet 20034390: ge_process_ipc_data_msg 207eeac8: lp_ipc_task 00040158: sys_end_task		
Condition:	1. Port has to be configured as a tagged port in the VPLS VLAN. 2. Delete the port from the VPLS VLAN using this CLI "no tagged eth <slot/port>".		

Issue ID:	NI-14153		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.2.00	**Technology:**	ACLs - Access Control Lists
Symptom:	IPv6 ACL accounting doesn't include PBR routed packets.		
Condition:	Configure IPv6 PBR with the set clause as "interface null0".		

Issue ID:	NI-14244		
Priority:	P4 - Low	**Severity:**	S4 - Low
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.0.00d	**Technology:**	PBR - Policy-Based Routing
Symptom:	GTP-u packet with L3 header as IPv4 and L4 header as IPv6 not forwarded with the IPv6 PBR on GTP port.		
Condition:	Configure IPv6 PBR and enable ingress-inner-filter on GTP port.		
Workaround:	Configure any IPv4 PBR with IPv6 PBR and bind it to the same GTP port.		

Issue ID:	NI-14265		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.0.00d	**Technology:**	SSH - Secure Shell
Symptom:	SSH Authentication may fail sometimes.		
Condition:	Using RSA public key authentication.		

Issue ID:	NI-14272		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported in Release:	NI 06.0.00d	**Technology:**	Hardware Monitoring
Symptom:	A 10G interface runs at 1G speed.		
Condition:	Specific to 20x10G line card when a port is configured for loop back system.		

Issue ID:	NI-14279		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	NI 06.0.00d	**Technology:**	LAG - Link Aggregation Group
Symptom:	LAG Load balancing may not be observed for GTP-c packets.		
Condition:	1) GTP has to be enabled on the port 2) GTP-c TEID hashing should be enabled		

Issue ID:	NI-14286		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00d	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	Routes through dead DR Other Router stays reachable in DR OSPFv3.		
Condition:	DR Other Router goes down/disabled.		
Workaround:	Wait for MaxAge to remove dead router's LSAs.		

Issue ID:	NI-14293		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00d	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	OSPFv3 and IPV6 neighborship not formed with remote VPLS peer.		
Condition:	Remote vpls peer configured with IPv6 on OSPFv3 interface with MPLS ttl policy applied.		
Workaround:	Either of the following can be applied 1. Remove the commands 'vrf-propagate-ttl and label-propagate-ttl enabled' under 'router mpls' configurations or 2. Configure static ipv6 neighbors		

Issue ID:	NI-14300		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.0.00d	**Technology:**	IPsec - IP Security
Symptom:	User may observe that IPSEC tunnel goes down and doesn't recover to up state.		
Condition:	User may observe this on a system with scaled IPSEC configuration.		

Issue ID:	NI-14354		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Security
Reported in Release:	NI 06.2.00	**Technology:**	ACLs - Access Control Lists
Symptom:	Loss of connectivity and ARP is not resolved.		
Condition:	1. MLX is upgraded to 6.0a and above versions with 4x10G module. 2. L4 deny all ACL applied on the physical interface as given below: ip access-list extended ABC permit ip x.0.0.0 0.0.0.y any deny ip any any interface ethernet a/b enable ip address x.0.0.z/y ip access-group ABC in		

Issue ID:	NI-14361		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Traffic Management
Reported in Release:	NI 06.2.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Burst traffic may be forwarded more than the configured rate on CES/CER.		
Condition:	Bursty traffic with Rate-limit is configured on the interface.		

Issue ID:	NI-14422		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Following error messages may be observed on MLX in Line card console:- kbp_duplicate_entry_IPVPN[0] idx : 0x00200bee tbl_id : 32 vpn_id = 4099, pfx : x.y.0.0/32.		
Condition:	On the reception of route update message for /32 prefix which matches local IP's network part.		

Issue ID:	NI-14436		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	IPv6 BGP peering session may encounter "Optional attribute error".		
Condition:	1. IPv6 Additional-Paths option is enabled 2. Processed withdraw message from neighbor		

Issue ID:	NI-14457		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	IP Multicast
Reported in Release:	NI 06.0.00f	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Multicast traffic forwarding may fail on MLX with High LP CPU.		
Condition:	When source traffic moves to a different port on same VE.		

Issue ID:	NI-14464		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	ICMP - Internet Control Message Protocol
Symptom:	IPv6 traffic may not be forwarded to destined port.		
Condition:	Specific to IPv6 Hop-by-hop and fragmented packets.		
Workaround:	Frequency of this issue can be lowered by configuring maximum value in the below configuration command "ipv6 nd reachable-time <secs>"		

Issue ID:	NI-14472		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported in Release:	NI 06.0.00f	**Technology:**	Hardware Monitoring
Symptom:	'show optic <slot>' does not show any light levels.		
Condition:	It is specific to third-party QSFP28-CFP2 optic.		

Issue ID:	NI-14479		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 06.0.00f	**Technology:**	CLI - Command Line Interface
Symptom:	'show chassis' displays power supply status as "Installed (Failed or Disconnected)" instead of "Installed (Shutdown)".		
Condition:	When 2100W power supply is manually powered off using command 'power-off power-supply #'.		

Issue ID:	NI-14486		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	BGP multipaths are not happened properly for BGP IPv6 routes that are learned in VRF.		
Condition:	1. iBGP neigborship established with 2 neighbors in VRF 2. BGP multipaths are enabled 3. The same route is advertised from both the neighbors with the same local_pref, MED, ORIGIN, weight		
Workaround:	Configure "always-compare-med" in 'router bgp'		

Issue ID:	NI-14504		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	include options in show command may not work as expected For instance:- Device#show ip bgp sum | i .8.9=> doesn't find the matching IP Device#show ip bgp sum | i .8.8.9 1.8.8.9 41617 ESTAB 0h 0m51s 0 1 116140 0		
Condition:	show command with pattern ".x.y", to match the IP such as "1.x.x.y".		

Issue ID:	NI-14596		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	NI 06.3.00	**Technology:**	LAG - Link Aggregation Group
Symptom:	For LACP based LAG deployment, device connected to NI device is not showing LAG member interface in down/Blocked state while NI device interfaces are LACP-Blocked.		
Condition:	This is a mis-configuration scenario where two or more interfaces connected to NI device in a LAG topology and one of member interface is incorrectly configured with different LAG Key.		
Workaround:	Configure same key on device connected to NI device.		

Issue ID:	NI-14625		
Priority:	P4 - Low	**Severity:**	S4 - Low
Product:	NetIron OS	**Technology Group:**	Monitoring
Reported in Release:	NI 06.2.00b	**Technology:**	Syslog
Symptom:	telnet client may not be observed in 'show logging' as configured.		
Condition:	'telnet client <ip-address>' is configured from a telnet session.		

Issue ID:	NI-14825		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	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.		

Issue ID:	NI-14826		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 05.8.00f	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	High CPU may be observed on CER.		
Condition:	Processed high rate of fragmented DHCP protocol packets.		

Issue ID:	NI-14827		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 05.8.00g	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF neighbors may show all ECMP paths after upgraded MLXe fails setting a forwarding address in AS External LSA.		
Condition:	It is rarely observed with the following steps:- (1) OSPFv2 is enabled on the device (2) static routes are configured with gateway, which is reachable and redistributed into OSPFv2 (3) Repeated image upgrade and downgrade		

Issue ID:	NI-14828		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 06.0.00f	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	IPv6 traffic may not be forwarded over VEoVPLS interface		
Condition:	MPLS LSP primary path goes down on disabling the VEoVPLS interface		
Workaround:	clear mpls lsp <lsp-name>		

Issue ID:	NI-14836		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	MPLS
Reported in Release:	NI 06.2.00b	**Technology:**	IP over MPLS
Symptom:	Traffic is not forwarded from default VRF to non-default VRF		
Condition:	1. Leak the Route between default and non-default VRF 2. MPLS tunnel starts from non-default VRF 3. Routes learnt via MPLS LDP tunnel in non-default VRF		

Issue ID:	NI-16478		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Management
Reported in Release:	NI 05.4.00b	**Technology:**	CLI - Command Line Interface
Symptom:	Active Management Module may unexpectedly reload with the following stack trace:- 2018052c: print_prompt(pc) 2017d6e0: print_prompt(lr) 2031f718: prompt_and_reprint 20390ac4: internal_release_page_mode 20390c2c: release_page_mode 2038fa90: parse_input 2094b848: ssh_event_handler 2095a0e8: ProcessChannelData 20958304: ShProcessMessage 2095f664: ProcessClientInputData 2095eed8: ShFiniteStateMachine 208845a0: HandleProtocolAction 20884d84: HandleReceive 20884ca4: HandleWaitingForReceive 20884448: HandleConnectionTask 2094a5bc: ssh_connection_task 2094ad3c: ssh_socket_control 2094d4b4: ssh_receive_data_ready 2094d4f8: ssh_tcp_receive_data_ready_callback 20a24f54: itc_process_msgs_internal 20a2528c: itc_process_msgs 20946a04: ssh_in_task 00005e18: sys_end_task		
Condition:	Configure "ntp-interface ve" command for VE interface id with higher value		

Issue ID:	NI-16573		
Priority:	P3 - Medium	**Severity:**	S3 - Medium
Product:	NetIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	NI 05.4.00e	**Technology:**	IP Addressing
Symptom:	Management port accepts packets corresponding to the same subnet of the lowest IPv4 primary address only		
Condition:	On configuring multiple IPv4 primary address on management port		

Issue ID:	NI-17360		
Priority:	P2 - High	**Severity:**	S2 - High
Product:	NetIron OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	NI 06.0.00g	**Technology:**	VLAN - Virtual LAN
Symptom:	CES/CER may reload unexpectedly with the following stack trace:- 048ac78: vlanlp_is_port_untagged(pc) 2048ac74: vlanlp_is_port_untagged(lr) 2008152c: is_my_vir_mac 20081cec: puma_cpu_packet 2008319c: puma_packet_poll 2027dbf8: ppcr_recieve_packet 200bc388: metro_sys_loop 200b19f4: main 00040158: sys_end_task		
Condition:	It is very rarely observed with no specific trigger		

Closed with code changes R6.0.00g

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 07/11/2018 in NI 6.0.00g.

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

Defect ID:	DEFECT000638335		
Technical Severity:	High	**Probability:**	High
Product:	Extreme NetIron OS	**Technology Group:**	OSPF - IPv4 Open Shortest Path First
Reported In Release:	NI 05.8.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Routes for VEoVPLS in a VRF may not be resolved.		
Condition:	Routes for VEoVPLS in a VRF may not be resolved.		

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

Defect ID:	DEFECT000660088		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme NetIron OS	**Technology Group:**	BGP4 - IPv4 Border Gateway Protocol

Reported In Release:	NI 06.0.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Line card may reload unexpectedly with the following stack trace:- Possible Stack Trace (function call return address list) 21672168: memcpy(pc) 211fe30c: kbp_memcpy(lr) 20b5bf9c: kbp_npxxpt_compare_data 20b5b504: kbp_npxxpt_execute_req 20b5b300: kbp_npxxpt_service_reqs 21547c34: kbp_xpt_service_requests 21546500: kbp_dm_12k_cbwlpm 2152ca78: device_compare 2152dcd0: kbp_instruction_search 21599064: NlmNsTrie__CheckAndFixRpt 215990f8: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599114: NlmNsTrie__FindIptUnderRpt 21599180: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 21599190: NlmNsTrie__FindRptEntries 215992d4: NlmNsTrie__SearchAndRepairRpt 215a7988: kbp_ftm_search_and_repair_rpt 215881bc: kbp_lpm_db_advanced_search_and_repair 215bab14: kbp_device_advanced_fix_errors 21534f38: kbp_device_12k_fix_parity_errors 2152a538: kbp_device_fix_errors 20b5561c: netroute_ifsr_fix_errors 20ac956c: nlcam_ifsr_netroute_scan_errors 20ac8b90: nlcam_ifsr_fifo_poll 200058c0: perform_callback 200062c8: timer_timeout 00040160: sys_end_entry 0005e4a0: suspend 0005cf78: dev_sleep 00005024: xsyscall 207f3af4: main 00040158: sys_end_task		
Condition:	Rarely observed during the execution of 'clear BGP neighbor' command when software is trying to fix a CAM error at the same time		

Workaround:	To disable the soft repair feature through the CLI using the cam ifsr disable command.

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

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

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

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

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

Closed with code changes R06.0.00f

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 02/19/2018 in NI 6.0.00f.

Defect ID:	DEFECT000613781		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	OAM - Operations, Admin & Maintenance
Reported In Release:	NI 05.7.00	**Technology:**	Monitoring
Symptom:	"show interface" may not have reason for port down.		
Condition:	Ports are brought down because of all back plane fabric links down.		

Defect ID:	DEFECT000617890		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	OSPF - IPv4 Open Shortest Path First
Reported In Release:	NI 05.6.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Ospfv3 Intra area route may not be calculated, if there are multiple Intra area prefix originated by same advertising router.		
Condition:	More than one Intra area prefix lsa originated by single advertising router & any other intra area prefix lsa with different advertising router's LSA hash becomes same.		

Defect ID:	DEFECT000619399		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	BGP4 - IPv4 Border Gateway Protocol
Reported In Release:	NI 05.8.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Removing and adding "aggregate-address x.y.z.q summary-only" causes BGP not to select the aggregate route as BEST route and subsequently prevents route advertisement for the aggregate route.		
Condition:	BGP global protocol distance for local route is configured as 255 and the aggregate route is marked as BEST in BGP and advertised to peers before the no form of command: "aggregate-address x.y.z.q summary-only" is executed.		
Workaround:	Change BGP global protocol distance for local routes to a value other than 255(other accepted values 1-254) and clear all the BGP neighbor sessions.		

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

Defect ID:	DEFECT000632625		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	OSPF - IPv4 Open Shortest Path First
Reported In Release:	NI 05.6.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	A route exists in OSPF route table but the same route is not seen in RTM.		
Condition:	1) An OSPF destination is reachable through 2 INTRA AREA paths on which, one of them is DIRECT and the other is reachable through a next-hop. (2) By executing the following sequence of commands through script Example: conf t int e 1/8 disable exit no int ve 124 Where, the interface e 1/8 is part of VE 124 and OSPF is configured on VE 124.		
Workaround:	Executing the following sequence of commands manually will avoid this issue Example: conf t int e 1/8 disable exit no int ve 124		

Defect ID:	DEFECT000634069		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	CLI - Command Line Interface
Reported In Release:	NI 05.9.00	**Technology:**	Management
Symptom:	Port of 20X10G Line card Module may not come up.		
Condition:	It is very rarely observed when a new connection is made on a port of 20X10G.		
Recovery:	Any one of the following methods can help in recovery:- 1. Removal and Re-insert of SFPP 2. Swap SFPP by SFP and re-swap SFP by SFPP. 3. Reload Line card Module.		

Defect ID:	DEFECT000637097		
Technical Severity:	High	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	BGP4 - IPv4 Border Gateway Protocol
Reported In Release:	NI 06.1.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	BGP session in VRF does not come up if the BGP session is trying to establish in non-default vrf instance which is on loop-back interface and the next-hop is configured on default vrf to reach the bgp peer.		
Condition:	BGP session on vrf instance is not coming up under the following conditions. 1) The BGP interface and the next-hop interfaces are not in the same vrf-forwarding instances. 2) Also when we configured inter vrf leaking for importing the routes.		
Workaround:	Follow all steps below to workaround the issue 1) Configure a secondary path to reach the BGP peer via different next-hop in the DUT. 2) The next-hop should be configured on the same vrf instance where the BGP session is originated in the DUT. 3) Also have the configuration to import the routes from one vrf to other vrf to achieve the inter-vrf routing configuration in the DUT.		

Defect ID:	DEFECT000639485		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	Traffic Queueing and Scheduling
Reported In Release:	NI 05.4.00	**Technology:**	Traffic Management
Symptom:	The EnQue/DeQue packet counts from "show tm-voq-stat src_port x/y cpu-queue" command does not match statistics of destination port		
Condition:	For all CPU destined traffic		

Defect ID:	DEFECT000640363		
Technical Severity:	Critical	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	PIM - Protocol-Independent Multicast
Reported In Release:	NI 05.6.00	**Technology:**	IP Multicast
Symptom:	Management Module unexpectedly reloads with the below stack trace and goes into a rolling reboot state :- Possible Stack Trace (function call return address list) 20f736f4: pack_pim_nbr_node(pc) 20f736f0: pack_pim_nbr_node(lr) 20f73bb4: process_pim_nbr_download_request 202cc074: process_dy_download_request 202b5e98: ipc_process_messages 202b6b4c: ipc_receive_packet 20d6e9f0: sw_receive_packet 20d6f4e8: mp_rx_main 00005e18: sys_end_task		
Condition:	It is very rarely observed during replacement of defective Line card Module		
Recovery:	1.Power-off the chassis 2. Remove one Management Module 3.Power-on the chassis and bring the first Management Module Up 4.Insert the other Management Module		

Defect ID:	DEFECT000640634		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	NI 06.0.00	**Technology:**	Layer 2 Switching
Symptom:	MCT cluster node fails to forward the packet towards CCEP ports		
Condition:	1. MCT cluster peer is down 2. Reload the Stand alone MCT cluster node		
Recovery:	Reconfigure the cluster by "no deploy/deploy".		

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

Defect ID:	DEFECT000642897		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	VRRPv3 - Virtual Router Redundancy Protocol Version 3
Reported In Release:	NI 06.0.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Ping failure is observed for a IPv6 VRRP virtual IP from Host.		
Condition:	1. VRRP master failover by disabling the VE interface 2. Bring back the VRRP node as master again by enabling the VE interface Example config: interface ve xx ip address a.b.c.d/24 ipv6 address e::f/64 ipv6 enable ipv6 vrrp vrid yy owner ipv6-address zz::a ipv6-address e::f activate !		
Recovery:	Ping from IPV6 VRRP master to Host to make reverse ping work.		

Defect ID:	DEFECT000643135		
Technical Severity:	Low	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	CLI - Command Line Interface
Reported In Release:	NI 05.8.00	**Technology:**	Management
Symptom:	Fan-threshold command does not display option for Gen 2 LIne card Modules though it accepts when executed.		
Condition:	When fan-threshold command is queried for further option.		

Defect ID:	DEFECT000644003		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	IP Addressing
Reported In Release:	NI 05.8.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	Ping fails on a newly configured VRRP node.		
Condition:	It is very rarely observed when a new VRRP instance is configured through a script on a telnet console Note: This is specific to CES/CER only. Example config: conf t vlan abc name XXX tagged ethe 2/3 to 2/4 router-interface ve abc interface ve abc port-name YYY ip address a.b.c.d/24 ip vrrp auth-type simple-text-auth xyz ip vrrp vrid abc owner ip-address a.b.c.d activate exit exit		
Recovery:	Disable and re-enable the VE conf t int ve abc disable enable end		

Defect ID:	DEFECT000644369		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	SNMP - Simple Network Management Protocol
Reported In Release:	NI 05.6.00	**Technology:**	Management
Symptom:	SNMP OID: "ifCounterDiscontinuityTime" does not have correct value.		
Condition:	SNMP polling for the OID: "ifCounterDiscontinuityTime".		

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

Defect ID:	DEFECT000645207		
Technical Severity:	Critical	**Probability:**	High
Product:	Brocade NetIron OS	**Technology Group:**	MPLS Traffic Engineering
Reported In Release:	NI 05.8.00	**Technology:**	MPLS
Symptom:	On a scaled scenario where the LSPs are adaptive and protected, when an interface which has a lot of LSPs, around a 1000 at least, goes down all these LSPs will attempt to establish MBB LSP at the same time which causes a spike in CPU usage. In some cases some of the LSPs might even go down due to lack of CPU availability to process control packets.		
Condition:	This happens only in scaled scenarios where the LSPs are adaptive and protected, and a few thousand such LSPs are riding a protected interface, and the protected interface goes down.		

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

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

Defect ID:	DEFECT000646510		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	RAS - Reliability, Availability, and Serviceability
Reported In Release:	NI 06.0.00	**Technology:**	Monitoring
Symptom:	Unable to configure "speed-duplex 100-full" on CES/CER 1G port.		
Condition:	On Optics E1MG-100BXD and E1MG-100BXU.		

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

Defect ID:	DEFECT000646997		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade NetIron OS	**Technology Group:**	ACLs - Access Control Lists
Reported In Release:	NI 05.7.00	**Technology:**	Security
Symptom:	Existing as-path access-list is modified when another access-list with same pattern is added.		
Condition:	Existing as-path access-list is modified when another access-list with same pattern and different sequence number is added like below:- Existing config: ip as-path access-list filter-from-as58453 seq 1 permit _xy$ ip as-path access-list filter-from-as58453 seq 10 deny _(xy[0-9])_ ip as-path access-list filter-from-as58453 seq 1000 permit ^.*$ New : 'ip as-path access-list filter-from-as58453 seq 2 deny ^.*$' The new rule modifies the existing rule with seq num 1000, as they have similar pattern string and hence, changes the action from permit to deny like below:- ip as-path access-list filter-from-as58453 seq 1000 deny ^.*$		

Defect ID:	DEFECT000648703		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade NetIron OS	**Technology Group:**	OSPF - IPv4 Open Shortest Path First
Reported In Release:	NI 06.2.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	OSPF may be installing invalid routes upon receiving invalid LSA		
Condition:	OSPF is flooded with invalid manipulated LSA and gets installed in database		

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Closed with code changes R06.0.00e

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 11/8/2017 in NI 6.0.00e.

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

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

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

Defect ID: DEFECT000651950	
Technical Severity: Medium	**Probability:** Low
Product: Brocade NetIron OS	**Technology Group:** Management
Reported In Release: NI 06.0.00	**Technology:** CLI - Command Line Interface
Symptom: Management Module may unexpectedly reload with the following stack trace:- Possible Stack Trace (function call return address list) 54797064: (pc) 20ac71d8: cu_show_int_lag_callback(lr) 20ad8e04: cu_show_int_lag 2044cc58: show_int_lag_all 202e8754: call_action_func 202e924c: parse_node 202e8cc8: parse_node_recurse 202e9514: parse_node 202e8cc8: parse_node_recurse 202e9514: parse_node 2035cd28: parse_input 2041c358: cli_aaa_accounting_callback 207906c0: aaa_accounting_start 2041bbac: cli_request_command_accounting 202e913c: parse_node 202e7790: parser 2035cd04: parse_input 20a94a74: ssh_event_handler 20aa7ccc: ProcessChannelData 20aa52e8: ShProcessMessage 20aae688: ProcessClientInputData 20aade20: ShFiniteStateMachine 209b03cc: HandleProtocolAction 209b01ac: HandleConnectionTask 20a93644: ssh_connection_task 20a93d90: ssh_socket_control 20a96a2c: ssh_receive_data_ready 20a96a70: ssh_tcp_receive_data_ready_callback 20b9321c: itc_process_msgs_internal 20b9	
Condition: "Show interface lag" is executed frequently from one or more SSH sessions.	

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

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