

MULTI-SERVICE IRONWARE SOFTWARE R05.6.00F FOR BROCADE MLX SERIES AND NETIRON FAMILY DEVICES Release Notes

Document History

Version of Document	Summary of Changes	Publication Date
R05.6.00f	Initial Release	4 February, 2015

© 2015 Brocade Communications Systems, Inc. All Rights Reserved.

ADX, AnyIO, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and HyperEdge, The Effortless Network, and The On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Contents

Overview of enhancements and configuration notes	5
Summary of 5.6.00f enhancements and configuration notes	5
Summary of 5.6.00e enhancements and configuration notes	5
Summary of 5.6.00d enhancements and configuration notes	6
Summary of 5.6.00c enhancements and configuration notes.....	7
Summary of 5.6.00b enhancements and configuration notes	8
Summary of 5.6.00a enhancements and configuration notes	8
Summary of 5.6.00 enhancements and configuration notes	9
Deprecated commands and features	25
Supported hardware	25
Supported devices	25
Supported blades	26
Interface modules	26
Brocade module compatibility matrix	28
Supported power supplies	29
Brocade MLX and Brocade NetIron XMR routers	29
Supported optics.....	29
Software or image filenames	30
Brocade MLX Series and NetIron XMR devices.....	30
NetIron CES and NetIron CER devices.....	32
Licensing information.....	33
System requirements	33
Configuration considerations	33
Limitations and restrictions	33

Router modules.....	33
Cryptographic updates	33
Upgrade and migration considerations	34
Hitless upgrade support	34
Upgrading to this release	34
Downgrading to a previous release.....	34
User guides.....	35
List of documents.....	35
Documentation updates	36
Reporting errors in the guides	36
Technical support.....	36
Getting technical help	36
Closed defects with code changes in R05.6.00f	37
Closed defects with code changes in R05.6.00e version 2	39
Closed defects with code changes in R05.6.00e.....	40
Closed defects with code changes in R05.6.00d.....	50
Closed defects with code changes in R05.6.00c	64
Closed defects with code changes in R05.6.00b.....	75
Open Defects in R05.6.00a	79
Closed defects without code changes in R05.6.00a.....	85
Closed defects with code changes in R05.6.00a.....	91
Open Defects in R05.6.00	122
Closed defects without code changes in R05.6.00	128
Closed defects with code changes in R05.6.00.....	136

Overview of enhancements and configuration notes

Summary of 5.6.00f enhancements and configuration notes

NOTE: There are no new features included in R05.6.00f.

Summary of 5.6.00e enhancements and configuration notes

The following table describes the new R05.6.00e features and the supported Brocade devices.

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
Poodle Vulnerability	Support for SSL 3.0 has been disabled due to protocol vulnerability. TLS 1.0 is the only support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP loss of sync message	The NTP Loss of Sync message has been updated to include the last synchronized device source.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
40G QSFP LM4 optics support	40 Gigabit Ethernet links over duplex multimode fiber, compliant with the QSFP+ MSA1,2 and represent a multimode adaptation of IEEE 802.3ba 40GBASE-LR4	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No advertising of Inter-VRF-leaked routes	This feature simplifies route-map configuration. An additional filtering mechanism has been added.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AES-CTR encryption support	<ol style="list-style-type: none"> 1. Reorder the AES modes to give preference to CTR mode over CBC on SSH connection 2. Keep CBC mode for backward compatibility with existing SSH clients that only support CBC mode 	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow-control mechanism enhancement	To prevent CRC errors observed on some connected ports of an MLX.	Yes	Yes	No	No	No	No	No
2x100 XPP ILKN monitoring	This feature monitors CRC errors in the Interlaken link/interface between XPP1 and XPP2 in 2 packet processors for the 2x100G card.	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Summary of 5.6.00d enhancements and configuration notes

The following table describes the new R05.6.00d features and the supported Brocade devices.

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
TM XPP link status check	TM XPP link is monitored periodically to identify issues between links and perform appropriate recovery.	Yes	Yes	No	No	No	No	No
Support for ESR4 optics	QSFP+ eSR4 Pluggable, Parallel Fiber-Optics Module for 40 Gb and 10 Gb Ethernet Applications.	Yes	Yes	No	No	No	No	No
FIPS Common Criteria: TLS Server Certificate Validation	Support for TLS Server Certificate validation in FIPS common-criteria mode of operation.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow control handling enhancements	Command added to provide the option to revert to the original behavior.	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Summary of 5.6.00c enhancements and configuration notes

The following table describes the new R05.6.00c features and the supported Brocade devices.

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
IPv6 packets on Openflow L23 port	When Openflow flow with matching L2 fields on an Openflow L23 hybrid port is present, this feature allows matching L2 field including IPv6 and forwarding traffic as per flow.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Simplified Upgrade and LP Auto-upgrade enhancement	This feature simplifies the upgrade process into a single CLI command. It uses the official release manifest file as an input. This feature also allows the system to be able to automatically upgrade a newly plugged in interface module.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Enhancement to predict Ratelimit sequence numbers as the configuration changes.	Maps each object of rate limit counter table entries to their corresponding ACL or VLAN or VLAN Group ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TM RAS Enhancements: TM DRAM CRC error interrupt, Descriptive TM error interrupt logging, Separate Threshold for CRC logging	This RAS feature monitors DRAM CRC errors on TM and takes appropriate action. It includes additional details in the display of TM/SFM fabric link error interrupt logs. It also includes new threshold support for logging fabric link CRC errors for both TM and SFM through CLI commands.	Yes	Yes	No	No	No	No	No
OpenSSL	Open SSL library update with support for RSA 2048 bit key with SHA-256 hashing algorithm, FIPS 186-3 standard and removal of heartbeat extension	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Summary of 5.6.00b enhancements and configuration notes

NOTE: There are no new features included in R05.6.00b.

Summary of 5.6.00a enhancements and configuration notes

The following table describes the new R05.6.00a features and the supported Brocade devices.

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
MP Presence from LP Detection (Headless Router Operation)	The LP maintains the MP state and brings itself down in case no MPs are present.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Configuring Management Interface under a user defined VRF	This feature allows you to add a management interface to a VRF instance of your choice.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enable FEC by default for MLXe4 and MLXe8	Forward Error Correction (FEC) mode enabled modules on a Brocade MLXe series chassis will reduce packet drops due to CRC errors.	Yes	Yes	No	No	No	No	No

Summary of 5.6.00 enhancements and configuration notes

The following table describes the new R05.6.00 features and the supported Brocade devices.

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
Brocade MLXe 4-Port 40 GbE - M Module	Brocade MLXe 4-port 40 GbE (M) module with Layer 2/IPv4/IPv6/MPLS/OpenFlow features, supports 512K IPv4 routes in the FIB. Requires high speed switch fabric modules and QSFP+ optics. For more information, refer to the <i>Brocade MLXe Hardware Installation Guide</i> .	No	Yes	No	No	No	No	No
Multipoint Static ARP and Static MAC Addresses for the CES/CER	The static ARP feature set is extended to forward Layer 3 unicast packets to multiple ports using multipoint static ARP entries, and the static MAC feature set is extended to forward Layer 2 packets to multiple ports in a VLAN using multipoint static MAC addresses for the Brocade NetIron CES/CER. For more information, refer to the Configuring IP chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	No	No	Yes	Yes	Yes	Yes	Yes
IPv4 Static Route over RSVP LSP	The IP/MPLS core routing feature set is enhanced with support for configuring IPv4 static routes next-hops as RSVP LSPs. ECMP up to 32 paths is supported. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	No	No	No	Yes
Entity MIB	The SNMP feature set is enhanced with support for the Entity MIB version 3 to manage multiple logical and physical entities. The entPhysicalTable, entPhysicalContainsTable, entLastChangeTime objects and entConfigChange trap are provided as defined in RFC 4133. For more information, refer to the Supported Standard MIBs chapter of the <i>Brocade Unified MIB Reference</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
IS-IS Graceful Restart "Helper Mode"	The core routing feature set is enhanced with support for IS-IS restart signaling as defined in RFC 5306 for a non-(re)starting router, also commonly referred to as "helper mode". IS-IS graceful restart enables a Brocade router to assist a restarting neighbor by continuing to forward traffic to it during its restart, so that the neighbor's restart is a hitless event. For more information, refer to the IS-IS (IPv4) chapter of the <i>Multi-Service IronWare Routing Configuration Guide</i> .	Yes	Yes	No	Yes	Yes	Yes	Yes
BFD Hardware Assist for the CES/CER	The BFD feature set for the Brocade NetIron CES/CER is enhanced with support to use hardware assist for transmitting BFD packets at sub-150 ms intervals for fine-grained neighbor forwarding detection. For more information, refer to the BFD chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	No	No	No	Yes	Yes	Yes	Yes
BFD Holdover for OSPF and IS-IS	The BFD feature set holdover mechanism is extended to OSPFv2, OSPFv3, and IS-IS for IPv4 and IPv6. BFD holdover timers are designed to minimize the disruption to routing protocols due to brief flapping of BFD sessions, and provide a configurable holdover timer for each routing protocol that suppresses BFD notifications during this interval. NetIron software release 5.0 supports BFD holdover for BGP. For more information, refer to the BFD chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	Yes	Yes	No	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
IPv6 Receive ACLs	The security feature set that provides hardware-based filtering of traffic destined to the router (receive ACLs) is extended with support for IPv6. In addition, named receive ACLs for both IPv4 and IPv6 are now supported. For more information, refer to the Access Control List and IPv6 Access Control List chapters of the <i>Multi-Service IronWare Security Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
Maximum Metric for OSPFv3 Router LSAs	The IP core routing feature set is extended to enable OSPFv3 to advertise its locally generated router LSAs with a maximum metric to direct transit traffic away from the router, while still routing for directly connected networks. For more information, refer to the OSPFv3 chapter of the <i>Multi-Service IronWare Routing Guide</i> .	Yes	Yes	No	No	Yes	Yes	Yes
LDP Outbound FEC Filtering	The MPLS core routing feature set is extended to support LDP outbound FEC filtering using prefix-lists, which provides the ability to control which FECs can be advertised to LDP neighbors. Previous software releases supports LDP inbound FEC filtering. For more information, refer to the MPLS LDP chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
127-Bit IPv6 Interface Addresses	The IPv6 address feature set is extended to use 127-bit IPv6 prefix lengths (/127) on inter-router point-to-point links as described in RFC 6164. For more information, refer to the Basic IPv6 Connectivity chapter of the <i>Multi-Service IronWare Routing Configuration Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
IPv6 ACL-Based Rate Limiting	The rate limiting feature set is extended to limit the rate of IPv6 traffic on an individual physical port that matches the permit conditions of an IPv6 ACL. For more information, refer to the Configuring Traffic Policing for Brocade NetIron XMR and Brocade MLX Series chapter of the <i>Multi-Service IronWare QoS and Traffic Management Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
RSVP Liberal Bypass LSP Selection	The MPLS core routing feature set for RSVP FRR is enhanced with an option to select a liberal set of criteria for facility backup path computation. Previous software releases support a restrictive set of criteria. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
sFlow Support for MPLS LSR and LER Interfaces	The sFlow implementation for real-time traffic analysis is extended to support sFlow monitoring for MPLS LSR and LER interfaces. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Link Protection Request for RSVP Fast Reroute	The MPLS core routing feature set for RSVP FRR is extended to support link protection request signaling for RSVP LSPs as described in RFC 4090. Previous software releases always signal node protection. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
MCT Client Scalability Enhancement	The Multi-Chassis Trunking (MCT) feature set for LAG redundancy is enhanced to support 512 clients (a switch or server connected to the MCT peers using a LAG). Previous software versions support 256 clients.	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
RSVP Hello Messages for Neighbor Failure Detection	The MPLS core routing feature set for RSVP is enhanced to support detecting neighbor failures using RSVP Hello messages as a keepalive mechanism between RSVP neighbors, as described in RFC 3209. For more information, refer to the MPLS LDP chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
Simplified Software Installation Optimization	The simplified software installation process that performs full system software installation with a single CLI command is optimized by introducing a version check of the line module FPGA images to determine whether it is necessary to download and install the image. Previous software releases always download the images, which can make software upgrade times longer than necessary. For more information, refer to the Simplified Upgrade chapter of the <i>Multi-Service IronWare Upgrade Guide</i> .	Yes	Yes	No	No	No	No	No
Max VPLS LSP Load Balance Scale for LER	The VPLS feature set for providing Metro and Carrier Ethernet services is extended to support VPLS load balancing over up to eight LSPs. Previous software releases support a maximum of four LSPs. For more information, refer to the MPLS VPLS chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
Simplified Line Module Troubleshooting	The RAS feature set is simplified with the CLI command "show np debug-stats" to display network processor troubleshooting statistics for any line module from an interactive session on the control module. The brocadeNPTMStatsMIB SNMP MIB is extended with the brcdNPDebugStatTable table. For more information, refer to the System DRAM chapter of the <i>Brocade Unified MIB Reference</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
RSVP TE Link Metric for CSPF Computation	The MPLS core routing feature set for RSVP traffic engineering is enhanced with support for a TE link metric that can be configured on an interface in addition to the IGP link metric. The TE and IGP metrics can be used independently of each other in different CSPF calculations. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
RSVP Auto-Bandwidth with Absolute Threshold	The MPLS core routing feature set for managing bandwidth automatically on RSVP LSPs is enhanced with configurable absolute adjustment thresholds, underflow functionality and the ability to sample and show the bandwidth utilization history for an LSP. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
System Resource Histogram Enhancements for Memory Errors	The system resource histogram feature set for monitoring and troubleshooting system resource allocation and utilization is enhanced with functionality to monitor line module memory errors. Error messages are logged via Syslog and SMP traps, and the brcdNPStatsTable in the brocadeNPTMStatsMIB SNMP MIB is extended with new OIDs. For more information, refer to the Continuous System Monitor chapter of the <i>Multi-Service IronWare Administration Guide</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
40 GbE and 100 GbE LAG Scalability	The carrier trunks feature set for link aggregation is enhanced with higher scalability for 40 GbE and 100 GbE interfaces to support 64 LAGs. Previous software releases support a maximum of 16 LAGs for 100 GbE interfaces. In addition, 40 GbE and 100 GbE interfaces now share the same LAG resource table. For more information, refer to the Brocade NetIron XMR and Brocade MLX Series Link Aggregation chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
Line Module Rolling Reboot Avoidance	The RAS feature set is enhanced with a mechanism to prevent line module rolling reboots. If a line module fails to boot after three consecutive attempts due to hardware failure of an FPGA image mismatch, the line module is put into interactive mode and error messages are logged. Previous software releases allow a line module to attempt to boot indefinitely, which wastes system resources. For more information, refer to the Network Processor MIB Definition chapter of the <i>Brocade Unified MIB Reference</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
OpenFlow Scalability and Operational Enhancements	The OpenFlow feature set for Software-defined Networking (SDN) is enhanced with a new optimized architecture that will enable future feature support and higher scalability. OpenFlow show and "debug openflow opm" CLI commands have been extended for better monitoring and troubleshooting, and enabling OpenFlow is now supported on multiple ports with a single CLI command. For more information, refer to the Configuring OpenFlow section of the <i>Multi-Service IronWare SDN Guide</i> .	Yes	Yes	No	No	Yes	No	Yes
Show Technical Support MPLS Label CLI Command Enhancement	The RAS feature set is enhanced with the "show tech-support mpls label" CLI command to show troubleshooting information for an MPLS label. For more information, refer to the Technical Support Diagnostics chapter of the <i>Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide</i> .	Yes	Yes	No	No	No	No	No
Line Module Memory Error Monitoring	The RAS feature set is extended with automated memory error monitoring for components on line modules that have their own memory. The specific type of memory error and affected component is logged via Syslog, SNMP traps or both. For more information, refer to the <i>Brocade MLXe Hardware Installation Guide</i> .	Yes	Yes	No	No	No	No	No
Show "Technical Support" Multicast CLI Command Enhancement	The RAS feature set is extended with "show tech-support" CLI command options to enable collection of technical support output for Layer 2, IPv4 and IPv6 multicast routing protocols. For more information, refer to the Technical Support Diagnostics chapter of the <i>Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
BFD for Static Routes	The BFD feature set is enhanced with support for IPv4 and IPv6 static routes using single-hop or multihop BFD sessions. For more information, refer to the Configuring IP chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> and the Static IPv6 Route chapter of the <i>Multi-Service IronWare Routing Configuration Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenFlow Hybrid Port Mode for VPLS Instances	The OpenFlow feature set for Software-defined Networking (SDN) is enhanced with support for hybrid port mode with protected VLANs and unprotected VLANs on VPLS endpoint ports. For more information, refer to the Hybrid switch and OpenFlow Hybrid port mode section of the <i>Multi-Service IronWare SDN Guide</i> .	Yes	Yes	No	No	No	No	No
BFD for RSVP-TE LSPs for the CES/CER	The BFD feature set for the Brocade NetIron CES/CER is enhanced with BFD for RSVP-TE LSPs to receive forwarding path detection failure messages from BFD. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
BFD for OSPFv3 for the CES/CER	The BFD feature set for the Brocade NetIron CES/CER is enhanced with support for OSPFv3 to receive forwarding path detection failure messages from BFD. For more information, refer to the BFD chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	Yes	Yes	No	Yes	Yes	Yes	Yes
Max LDP ECMP at the Ingress LER	The MPLS core routing feature set is extended to support LDP ECMP to load balance traffic over up to eight LSPs at the ingress LER. Previous software release support a single path. For more information, refer to the MPLS LDP chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
ITU-T Y.1731 Loss Measurement for the CES/CER	The OAM feature set for providing Metro and Carrier Ethernet services on the Brocade NetIron CES/CER is extended to support ITU-T Y.1731 on-demand single-ended loss measurement (ETH-LM). Layer 2 VLANs, LAGs and VPLS endpoints are supported, VLLs are not supported. The Y.1731 MIB is also supported for remote management with SNMP. For more information, refer to the OAM chapter of the <i>Multi-Service IronWare Administration Guide</i> and the Supported Standard MIBs chapter of the <i>Brocade Unified MIB Reference</i> .	No	No	Yes	Yes	Yes	Yes	Yes
ACL Editing	The ACL functionality for filtering traffic is enhanced with sequence numbers that enable users to insert, modify or delete rules at any position, without having to remove and reapply the entire ACL. ACL editing is supported for MAC, IPv4 and IPv6 using standard, extended and named ACLs. For more information, refer to the Access Control List, Layer 2 Access Control Lists, and IPv6 Access Control List chapters of the <i>Multi-Service IronWare Security Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
OpenFlow Scaling Enhancement	The OpenFlow feature set for Software-defined Networking (SDN) is enhanced to support 32K flows on the Brocade NetIron CES/CER routers, 64K flows on the Brocade MLX router, and 128K flows on the Brocade XMR router. Previous software versions support 4K flows per router. For more information, refer to the OpenFlow Scaling section of the <i>Multi-Service IronWare SDN Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
OpenFlow Layer 2 and Layer 3 Matching	The OpenFlow feature set for Software-defined Networking (SDN) is enhanced with support for matching a combination of Layer 2 and Layer 3 rules. Previous software releases support either Layer 2 or Layer 3 rules, but not both at the same time. OpenFlow hybrid port mode, introduced in software version 5.5, is supported with Layer 2 and Layer 3 matching. For more information, refer to the Configuring OpenFlow section of the <i>Multi-Service IronWare SDN Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ND6 IPv6 Prefix Suppress	The IPv6 routing feature is enhanced to suppress the advertisement of on-link prefix information in the router advertisement (RA) messages in a LAN where multiple Hosts are connected to the Routers. This prevents hosts from auto configuring based on the prefix in the RA message and use DHCPv6 instead for security/accountability reasons. This is also helpful in suppressing the advertisement of identical prefixes by multiple routers. For more information, refer to the IPv6 Prefix List chapter of the Multi-Service IronWare Routing Configuration Guide.	Yes	Yes	No	Yes	Yes	Yes	Yes
L2 Multicast CPU Protection	The RAS feature set is introduced (*,G) based forwarding for snooping to relieve the MP CPU of numerous pending FID updates, and aging out OIFs. For more information, refer to <i>Multi-Service IronWare Multicast Configuration Guide</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
JITC, FIPS, USGv6, Common Criteria	<p>The Joint Interoperability Test Command (JITC) conducts testing of national security systems and information technology systems hardware, software and components. Services include developmental, conformance, interoperability, operational and validation testing. A Federal Information Processing Standard (FIPS) is a publicly announced standardization developed by the United States federal government for use in computer systems [1] by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract. USGv6.S. Government IPv6 (USGv6) Profile and subsequent testing program resulted from the directive to the National Institute of Standards and Technology (NIST) to develop the technical infrastructure necessary to support wide scale adoption of IPv6 in the US Government (USG).</p> <p>Common Criteria is an internationally recognized methodology for security evaluation and certification that is sanctioned by the International Standards Organization (ISO).</p>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PBR Policy Scaling Enhancements	The core routing feature set for PBR is enhanced to support 400 route-map policies. Previous releases support 64 policies.	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
IPv6 ACL Scaling Enhancement	The ACL functionality for filtering traffic is extended with support for 200 IPv6 ACLs. Previous software releases support 100 IPv6 ACLs. For more information, refer to the IPv6 Access Control List chapter of the <i>Multi-Service IronWare Security Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
Configurable TM Buffer Thresholds	The Quality of Service (QoS) feature set for traffic management is extended with configurable traffic manager (TM) buffer thresholds to increase throughput for bursty multicast traffic. For more information, refer to the Configuring Traffic Policing for Brocade NetIron XMR and Brocade MLX Series chapter of the <i>Multi-Service IronWare QoS and Traffic Management Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
Line Module Configuration Deletion in Interactive Boot Mode	Operational enhancements are made so that line module configurations can be deleted when a module is in interactive boot mode. For more information, refer to the ACL and QoS Diagnostics chapter of the <i>Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide</i> .	Yes	Yes	No	No	No	No	No
CLI Command to Delete OpenFlow Flows	The OpenFlow feature set for Software-defined Networking (SDN) is extended with a CLI command to manually delete OpenFlow flows in cases where the router and OpenFlow controller are out of synchronization. For more information, refer to the Administering OpenFlow section of the <i>Multi-Service IronWare SDN Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
Automatic Tuning of Links Between Line Modules and SFMs	The RAS feature set is extended with automatic monitoring and tuning of transmit and receive parameters on SERDES links between line modules and switch fabric modules (SFMs) that are down due to excessive CRC errors. For more information, refer to the Configuring Basic Parameters chapter of the <i>Multi-Service IronWare Administration Guide</i> .	Yes	Yes	No	No	No	No	No
VPLS Flooding and Broadcast Optimization	The VPLS feature set for providing Metro and Carrier Ethernet services is optimized for flooding and broadcast traffic replication in a VPLS instance. These functions are performed in a separate task on the line module processor to improve performance in large VPLS instances.	Yes	Yes	No	No	No	No	No
TVF and PBR to TVF LAG Load Balancing	The carrier trunks feature set for link aggregation is enhanced with LAG load balancing for traffic that is switch using transparent VLAN flooding. For more information, refer to the VLAN chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	Yes	Yes	No	No	No	No	No
PBR VLAN Preservation for the Brocade MLXe 24-Port 10 GbE (DM) SFP+ Module	The core routing feature set for PBR on the Brocade MLXe 24-port 10 GbE (DM) module is extended to support 802.1Q VLAN and 801.2p priority preservation when using the "preserve-vlan" policy option. Previous software releases support this feature on generation 1 and generation 2 modules. For more information, refer to the VLAN chapter of the <i>Multi-Service IronWare Switching Configuration Guide</i> .	Yes	Yes	No	No	No	No	No

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
FEC Mode on hSFM Links	Forward Error Correction (FEC) mode is enabled on switch fabric links on the Brocade MLXe-16 and MLXe-32 routers with 2-port 100 GbE (X), 4-port 40 GbE (M), and 24-port 10 GbE (DM) line modules and hSFM. FEC reduces the number of CRC errors and packet loss between the line modules and high-speed switch fabric modules. For more information, refer to the <i>Brocade MLXe Hardware Installation Guide</i> .	Yes	Yes	No	No	No	No	No
Debug Task CLI Command Enhancements	The RAS feature set for system task diagnostics is enhanced with the ability to only display debug output from the specified task on the console, Telnet session, SSH session or Syslog server. In addition, the debug output can be sent to a buffer in memory which can be displayed via a CLI command on an interactive login session. Previous software releases display debug output from multiple tasks which can be cumbersome to read. For more information, refer to the Using Diagnostic Commands chapter of the <i>Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide</i> .	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Runtime Diagnostics Scheduling	The RAS feature set is extended with the ability to schedule and display output from runtime diagnostic tests. The "sysmon" architecture and automated runtime diagnostic tests are implemented in software release 5.5.	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	Brocade NetIron XMR Series	Brocade MLX Series	Brocade NetIron CES 2000 Series BASE package	Brocade NetIron CES 2000 Series ME_PREM package	Brocade NetIron CES 2000 Series L3_PREM package	Brocade NetIron CER 2000 Series Base package	Brocade NetIron CER 2000 Series Advanced Services package
RSVP Global Configuration for Refresh Reduction and Reliable Messaging	The MPLS core routing feature set for RSVP is extended to support configuring RSVP refresh reduction and reliable messaging at the global level for the router, in addition to the interface level. Previous software releases support these configurations at the interface level. For more information, refer to the MPLS TE chapter of the <i>Multi-Service IronWare MPLS Configuration Guide</i> .	Yes	Yes	No	Yes	No	No	Yes
Line Module Shutdown if Both Control Modules Are Unavailable	The RAS feature set is extended with a mechanism to shutdown line modules in the event that both control modules are down or are removed from the chassis. In this situation the router will stop forwarding all traffic, and will avoid the possibility of hardware flooding or dropping control traffic that needs to be processed by the router. For more information, refer to the ACL and QoS Diagnostics chapter of the <i>Brocade MLX Series and Brocade NetIron XMR Diagnostic Guide</i> .	Yes	Yes	No	No	No	No	No
Mapping Syslog Messages to SNMP Notifications	The SNMP network management feature set is enhanced with support for the SNMP MIB and traps for mapping Syslog messages to SNMP notifications as defined in RFC 5676. The syslogMsgSDTable structured data table is not supported due to incompatibilities in the NetIron Syslog server implementations.	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Deprecated commands and features

No deprecated commands were included in this release.

Supported hardware

Supported devices

Table 1 describes the Brocade devices supported in this release.

Table 1 Supported Brocade devices

Brocade NetIron XMR Series	Brocade MLX Series	NetIron CES 2000 and NetIron CER 2000 Series
<ul style="list-style-type: none">• Brocade NetIron XMR 4000• Brocade NetIron XMR 8000• Brocade NetIron XMR 16000• Brocade NetIron XMR 32000	<ul style="list-style-type: none">• Brocade MLX-4• Brocade MLX-8• Brocade MLX-16• Brocade MLX-32• Brocade MLXe-4• Brocade MLXe-8• Brocade MLXe-16• Brocade MLXe-32	<ul style="list-style-type: none">• Brocade NetIron CES 2024C-4X• Brocade NetIron CES 2024F-4X• Brocade NetIron CER-RT 2024C-4X• Brocade NetIron CER-RT 2024F-4X• Brocade NetIron CES 2024C• Brocade NetIron CES 2024F• Brocade NetIron CES 2048C• Brocade NetIron CES 2048CX• Brocade NetIron CES 2048F• Brocade NetIron CES 2048FX• Brocade NetIron CER 2024C• Brocade NetIron CER-RT 2024C• Brocade NetIron CER 2024F• Brocade NetIron CER-RT 2024F• Brocade NetIron CER 2048C• Brocade NetIron CER-RT 2048C• Brocade NetIron CER 2048CX• Brocade NetIron CER-RT 2048CX• Brocade NetIron CER 2048F• Brocade NetIron CER-RT 2048F• Brocade NetIron CER 2048FX• Brocade NetIron CER-RT 2048FX

Supported blades

Interface modules

Interface modules for Brocade MLX, Brocade MLXe, and Brocade NetIron XMR routers are available in three types:

- Gen-1 interface modules

Note: In prior release notes, the NI-MLX-1GX48-T has been listed as a GEN1 module. It is actually a Gen 1.1 module.

- Gen-2 interface modules, which provide additional functionality, more memory, and higher operation speeds.
- Gen 3a interface modules, which provide higher port density (ASIC-based architecture)

Table 2 lists the interface modules that are supported for Brocade MLX Series and Brocade NetIron XMR routers in this release.

Table 2 Interface modules for all Brocade MLX Series and Brocade NetIron XMR routers

SKU	Ports	Description
NI-MLX-10GX2	2	NetIron MLX Series 2-port 10-GbE module with IPv4/IPv6/MPLS hardware support - requires XFP optics.
NI-XMR-10GX2	2	Gen-1 2-port 10-Gbps Ethernet module - requires XFP optics. IPv4, IPv6, MPLS support.
BR-MLX-100GX-1	1	MLXE/XMR/MLX 1-port 100-GbE (X) Module with IPv4/IPv6/MPLS hardware support - requires CFP optics. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode. Requires high speed switch fabric modules. License upgradable to 2-ports on an MLXe.
BR-MLX-100GX-2	2	MLXE 2-port 100-GbE (X) Module with IPv4/IPv6/MPLS hardware support requires CFP optics. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode. Requires high speed switch fabric modules.
BR-MLX-40Gx4-M	4	Brocade MLXe four (4)-port 40-GbE (M) module with IPv4/IPv6/MPLS hardware support - requires QSFP+ optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules
NI-MLX-10GX4	4	NetIron MLX Series 4-port 10-GbE module with IPv4/IPv6/MPLS hardware support - requires XFP optics.
NI-XMR-10Gx4	4	NetIron XMR Series 4-port 10-GbE module with IPv4/IPv6/MPLS hardware support - requires XFP optics.
BR-MLX-10GX4-X	4	XMR/MLXe 4-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support - requires XFP optics. Supports 1M IPv4 routes in FIB.
BR-MLX-10Gx4-X-ML	4	MLX/MLXe 4-port 10-GbE (ML) module with IPv4/IPv6/MPLS hardware support-requires XFP optics. Supports 512K IPv4 routes in FIB. License Upgradable to "X" scalability (1M IPv4 routes in FIB).

SKU	Ports	Description
NI-MLX-10GX8-M	8	Brocade MLX Series 8-port 10-GbE (M) module with IPv4/IPv6/MPLS hardware support - requires SFPP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules.
NI-MLX-10GX8-D	8	Brocade MLX Series 8-port 10-GbE (D) module with IPv4/IPv6 hardware support - requires SFPP optics. Supports 256K IPv4 routes in FIB. Does not support MPLS. Requires high speed switch fabric modules.
BR-MLX-10GX8-X	8	MLXe/XMR 8-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support-requires SFPP optics. Supports 1M IPv4 routes in FIB. Requires high speed switch fabric modules.
NI-MLX-1GX20-SFP	20	NetIron MLX Series 20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support - requires SFP optics. Note: Copper SFPs are supported at 1000Mbps only.
NI-XMR-1GX20-SFP	20	NetIron XMR Series 20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support - requires SFP optics. Note: Copper SFPs are supported at 1000Mbps only.
NI-MLX-1GX20-GC	20	NetIron MLX Series 20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.
NI-XMR-1GX20-GC	20	NetIron XMR Series 20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.
BR-MLX-1GCX24-X	24	XMR/MLXE 24-port 1-GbE (X) Copper (RJ-45) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.
BR-MLX-1GCX24-X-ML	24	MLX/MLXE 24-port 1-GbE (ML) Copper (RJ-45) Module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB. License Upgradable to "X" scalability (1M IPv4 routes in FIB).
BR-MLX-1GFx24-X	24	XMR/MLXE 24-port 1-GbE (X) Copper (RJ-45) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.
BR-MLX-1GFX24-X-ML	24	MLX/MLXE 24-port 1-GbE (ML) Fiber (SFP) Module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB. License Upgradable to "X" scalability (1M IPv4 routes in FIB).
BR-MLX-10GX24-DM	24	MLXE 24-port 10-GbE (up to 18 ports wire-speed) Module with IPv4/IPv6/MPLS hardware support - requires SFPP optics. Supports 256K IPv4 routes in FIB.
NI-MLX-1GX48-T-A	48	Gen 1.1 NetIron MLX Series 48-port 10/100/1000ase-T, MRJ21 module with IPv4/IPv6/MPLS hardware support. Requires high speed fans NIBI-16-FAN-EXH-A on MLX-16.

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, which means you can remove and replace them without powering down the system.

Brocade module compatibility matrix

Note: In prior release notes, the MLX 48x1G-T was listed as GEN1 module. It is actually a Gen 1.1 module.

Table 3 Brocade module compatibility matrix for MLXe, MLX, and XMR chassis

Module	MLX		XMR		MLXe with MLX or MR2-M mgmt module	MLXe with XMR or MR2-X mgmt module	Generation (G)
	SFM	hSFM	SFM	hSFM			
MLX 4x10G	Yes	Yes	No	No	Yes	No	G1
MLX 2x10G	Yes	Yes	No	No	Yes	No	G1
MLX 20x1G	Yes	Yes	No	No	Yes	No	G1
MLX 48x1G-T	Yes	Yes	No	No	Yes	No	G1.1
MLX 8x10G-D	No	Yes	No	No	Yes	No	G2
MLX 8x10G-M	No	Yes	No	No	Yes	No	G2
XMR 4x10G	No	No	Yes	Yes	No	Yes	G1
XMR 20x1G	No	No	Yes	Yes	No	Yes	G1
24x1G-X	Yes	Yes	Yes++	Yes++	Yes	Yes++	G1.1
24x1G-X-ML*	Yes	Yes	No	No	Yes	No	G1.1
4x10G-X	Yes	Yes	Yes++	Yes++	Yes	Yes++	G1.1
4x10G-X-ML**	Yes	Yes	No	No	Yes	No	G1.1
8x10G-X	No	Yes	No	Yes	Yes	Yes	G2
2x100G-X***	No	Yes	No	Yes	Yes	Yes	G2
1x100G-X****	No	Yes	No	Yes	Yes	Yes	G2
4x40G-M	No	No	No	No	Yes	Yes	G2
24x10G-DM	No	No	No	No	Yes	No	G3a

++ Requires "X" scalability license

*4x10G-X-ML can be converted to 4x10G-X with a license.

**24x1G-X-ML can be converted to 24x1G-X with a license

***Only one port of 2x100G-X can be used in MLX and XMR chassis.

****1x100G-X can be converted to a 2x100G-X with a license.

- For the latest and most up to date information on modules supported on MLXe, MLX and XMR chassis, log in to www.mybrocade.com and access the TECH NOTE: BROCADE MLX SERIES MODULE SUPPORT document.
 - Specific information regarding RAD optics configuration on the Brocade MLX Series and Brocade NetIron XMR platforms has been documented in the RAD optics Solutions test report. Please work with your account team to gain access to the document.
-

Supported power supplies

Brocade MLX and Brocade NetIron XMR routers

Table 4 lists the power supplies that are available for Brocade MLX and Brocade NetIron XMR routers.

Table 4 Power supplies

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

Supported optics

For a list of supported fiber-optic transceivers that are available from Brocade, refer to the latest version of the Brocade Optics Family Data Sheet available online at www.brocade.com.

Software or image filenames

Table 5 and Table 6 list the images required for R05.6.00f.

Brocade MLX Series and NetIron XMR devices

Table 5 Required images for a basic R05.6.00f software upgrade

```
-NETIRON_IRONWARE_VER XMR-MLXV5.6.00f
#=====
-DIRECTORY /Boot/InterfaceModule
xmlprm05600.bin
-DIRECTORY /Boot/ManagementModule
xmprm05600.bin
# Application Images
-DIRECTORY /Combined/FPGA
lpfpga05600f.bin
-DIRECTORY /Combined/Application
xm05600f.bin
-DIRECTORY /Monitor/InterfaceModule
xmlb05600.bin
-DIRECTORY /Monitor/ManagementModule
xmb05600.bin
-DIRECTORY /Application/ManagementModule
xmr05600f.bin
-DIRECTORY /Application/InterfaceModule
xmlp05600f.bin
-DIRECTORY /FPGA/InterfaceModule
pbif4x40_05600f.bin 1.03
pbif8x10_05600f.bin 2.16
pbifmrj_05600f.bin 4.02
pbifsp2_05600f.bin 4.02
statsmrj_05600f.bin 0.09
xgmacsp2_05600f.bin 0.17
xpp2x100_05600f.bin 6.09
xpp4x40_05600f.bin 2.05
xpp8x10_05600f.bin 7.04
xppmrj_05600f.bin 1.01
xppsp2_05600f.bin 1.01
xppxsp2_05600f.bin 1.01
-DIRECTORY /FPGA/ManagementModule
mbridge32_05600f.xsvf 36
mbridge_05600f.xsvf 37
sbridge_05600f.mcs 6
hsbridge_05600f.mcs 17

-END_OF_IMAGES

-DIRECTORY /Signatures
xmlprm05600.sig
xmprm05600.sig
xmlb05600.sig
xmb05600.sig
```

xmr05600f.sig
xmlp05600f.sig
lpfpga05600f.sig
hsbridge_05600f.sig
mbridge_05600f.sig
mbridge32_05600f.sig
sbridge_05600f.sig
pbif4x40_05600f.sig
pbif8x10_05600f.sig
pbifmrj_05600f.sig
pbifsp2_05600f.sig
statsmrj_05600f.sig
xgmacsp2_05600f.sig
xpp2x100_05600f.sig
xpp4x40_05600f.sig
xpp8x10_05600f.sig
xppmrj_05600f.sig
xppsp2_05600f.sig
xppxsp2_05600f.sig
xmlprm05600.sha256
xmprm05600.sha256
xmlb05600.sha256
xmb05600.sha256
xmr05600f.sha256
xmlp05600f.sha256
lpfpga05600f.sha256
hsbridge_05600f.sha256
mbridge_05600f.sha256
mbridge32_05600f.sha256
sbridge_05600f.sha256
pbif4x40_05600f.sha256
pbif8x10_05600f.sha256
pbifmrj_05600f.sha256
pbifsp2_05600f.sha256
statsmrj_05600f.sha256
xgmacsp2_05600f.sha256
xpp2x100_05600f.sha256
xpp4x40_05600f.sha256
xpp8x10_05600f.sha256
xppmrj_05600f.sha256
xppsp2_05600f.sha256
xppxsp2_05600f.sha256

NOTE: FPGA images are not needed for 24x10G modules.

NetIron CES and NetIron CER devices

Table 6 Required images for a basic R05.6.00f software upgrade

```
-NETIRON_IRONWARE_VER CES-CERV5.6.00f
#=====
-DIRECTORY /Boot
ceb05600c.bin
-DIRECTORY /Application
ce05600f.bin
-DIRECTORY /FPGA
pbifmetro_05600f.bin
-END_OF_IMAGES

-DIRECTORY /Signatures
ceb05600c.sig
ce05600f.sig
pbifmetro_05600f.sig
ceb05600c.sha256
ce05600f.sha256
pbifmetro_05600f.sha256
```

Licensing information

For a complete list of available software and port licensing, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

System requirements

For system requirements, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

Configuration considerations

For configuration considerations, refer to the latest version of the *Multi-Service IronWare configuration guides* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

Limitations and restrictions

For limitations and restrictions, refer to the latest version of the *Multi-Service IronWare configuration guides* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

- Customers with ACL and VPLS configuration on 2x100G cards should not upgrade to 5.6.00 or 5.6.00a. For details please refer to defect (DEFECT000487721).

Router modules

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

Cryptographic updates

FIPS: Replace NSS Cryptographic Engine with OpenSSL.

Note: OpenSSL has been compiled without the heartbeat extension, which means the version of OpenSSL in the Brocade code is not impacted by the “Heartbleed Vulnerability.”

FIPS: Update applications to use OpenSSL crypto engine for any cryptographic operation.

FIPS: Signatures to be generated using RSA 2048 and SHA-256 hash, instead of current DSA 1024.

The Key Exchange Algorithm used for SSH are:

- In non-FIPS, it is “diffie-hellman-group1-sha1”
- In FIPS, it is “diffie-hellman-group-exchange-sha256”
- In FIPS-CC mode, it is “diffie-hellman-group14-sha1”

Upgrade and migration considerations

For upgrade and migration considerations, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

Hitless upgrade support

For hitless upgrade support, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

NOTE: Hitless Upgrade from any release to R05.6.00f is NOT supported. Refer to the Multi-Service IronWare Software Upgrade Guide for R05.6.00f for details.

Upgrading to this release

For upgrade information, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

Downgrading to a previous release

For downgrade information, refer to the latest version of the *Multi-Service IronWare Software Upgrade Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

User guides

List of documents

Refer to <http://www.brocade.com/ethernetproducts> or my.brocade.com for the latest versions of the documents.

For easy navigation, the table below provides a mapping of the previous guides to the new set of Multi-Service IronWare documentation. Use the READ_ME_FIRST file in the NI_05600a_SWdocs.zip file for instructions on searching all the software manuals at once.

Previous guides	New Multi-Service IronWare manuals
Brocade MLX Series and NetIron Family Configuration Guide	Multi-Service IronWare Administration Configuration Guide
	Multi-Service IronWare Security Configuration Guide
	Multi-Service IronWare Switching Configuration Guide
	Multi-Service IronWare Routing Configuration Guide
	Multi-Service IronWare Traffic Management Configuration Guide
	Multi-Service IronWare Multicast Configuration Guide
	Multi-Service IronWare Multiprotocol Label Switch (MPLS) Configuration Guide
	Multi-Service IronWare Software Defined Networking (SDN) Configuration Guide
Brocade MLX Series and Brocade NetIron Family YANG Guide	Multi-Service IronWare YANG Guide
Brocade MLX Series and NetIron XMR Series Diagnostic Reference	Brocade MLX Series and NetIron XMR Series Diagnostic Reference
Unified IP MIB Reference	Unified IP MIB Reference
Multi-Service IronWare Software Upgrade	Multi-Service IronWare Software Upgrade Guide
Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide	Brocade MLXe Series Hardware Guide
	Brocade MLX Series and Brocade NetIron XMR Hardware Guide
Brocade NetIron CES and Brocade NetIron CER Devices Hardware Guide	Brocade NetIron CES Series and Brocade NetIron CER Series Hardware Guide
	Multi-Service IronWare Feature Support Matrix

Documentation updates

For documentation updates, refer to the latest version of the *Multi-Service IronWare Update Guide* on <http://www.brocade.com/ethernetproducts> or my.brocade.com.

Reporting errors in the guides

Send an email to documentation@brocade.com to report errors in the user guides.

Technical support

Contact your supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

- General information
- Technical Support contract number, if applicable
- Device model
- Operating system version
- Error numbers and messages received
- Detailed description of the problem, including the device or network behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Device serial number

Getting technical help

If you have a direct support contract with Brocade, go to <http://www.brocade.com/services-support/index.page> for the latest e-mail and telephone contact information.

Closed defects with code changes in R05.6.00f

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00f. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID. This list was closed on January 29, 2015.

Defect ID:	DEFECT000508661		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	System
Reported In Release:	NI 05.6.00	Technology Area:	Optics
Symptom:	On reload after upgrade to NI 05.6.00b, CRC errors increment on MLX ports connected to the switch/router.		
Condition:	Upgrade of MLX chassis with 8x10G modules to NI 05.6.00b.		

Defect ID:	DEFECT000530261		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.8.00	Technology Area:	LDP
Symptom:	The system experienced a software fault, leading to a restart of the management module.		
Condition:	The software fault may be experienced when there is a large scale VPLS and MPLS implementation ¹ , and the loopback address at one of the peers is repeatedly disabled and enabled. A race condition in the PWE3 download handling leads to some of the PWE3 events never being properly handled by the L2VPN module. As a result of the missing update(s) there is an unexpected data structure; eventually leading to the MP reboot.		

Defect ID:	DEFECT000536491		
Technical Severity:	High	Probability:	Low
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.4.00	Technology Area:	MPLS Traffic Engineering
Symptom:	In the case of an MPLS RSVP network with one to one backup FRR LSP sessions, management module can reset unexpectedly.		
Condition:	Some of the sessions for the LSP were stale entries because cleanup was not performed correctly. While processing the RSVP control message for a new session entry, the unexpected reload is seen.		
Recovery:	<p>This is a corner case in the RSVP area and the probability of occurrence is low. If this scenario is encountered, perform an MM switchover if a redundant MM is present or reload the router.</p> <p>As a result of the above:</p> <ul style="list-style-type: none"> - All MPLS tunnels originating/terminating at this router will go down and experience traffic loss until they are re-signaled. 		

Defect ID:	DEFECT000538328		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	BGP4 (IPv4)
Symptom:	Under certain conditions, a VPN route reflector may incorrectly send VPN route withdraws to its neighbors.		
Condition:	This may occur when a VPN router reflector receives a VPN route, and at the same time also originates the same VPN route.		

Defect ID:	DEFECT000539691		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	Other IPv4
Symptom:	VRRP, MCT, and OSPF stopped receiving protocol packets and stuck the LP CPU queue associated with TM on a 2x100G module.		
Condition:	Software upgrade with manifest file through TFTP.		

Defect ID:	DEFECT000540049		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	System
Reported In Release:	NI 05.6.00	Technology Area:	Component
Symptom:	When there is fiber cut in the primary path with FRR enabled, 300ms of switchover time to secondary is observed.		
Condition:	Primary and secondary path established with FRR enabled and fiber cut in the primary path		

Defect ID:	DEFECT000541113		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.2.00	Technology Area:	NTP - Network Time Protocol
Symptom:	Network Time Protocol (NTP) is affected with the following security vulnerabilities: CVE-2014-9293, CVE-2014-9294, CVE-2014-9295 and CVE-2014-9296. Only the last (CVE-2014-9296) affects NetIron code.		
Condition:	In NTP source code, a rare error case is missing a return statement resulting in a situation that may be exploitable by an attacker. 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.		
Workaround:	Disable authentication on both the NTP server and client modes.		

Defect ID:	DEFECT000541565		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	BFD
Symptom:	Configuring more than one static route with LSP as the nexthop leads to system reload.		
Condition:	(1) MPLS LSPs setup on the router (2) Presence of one static route with LSP as next hop		

Defect ID:	DEFECT000544803		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	BGP4+ (IPv6)
Symptom:	Upon clearing soft out for the VPNv4/v6 neighbor, BGP resends VPNv4/6 advertisements to the neighbor. While sending the advertisements, the local VRF route source should be preferred over the learned VPN route source. This tie break rule was not honored and both the VRF route source and the VPN route source were advertised, causing the unexpected system reboot.		
Condition:	Advertisement of the VPN route could come from either the local VRF source or the VPN neighbor source, i.e., the local router acting as a route reflector. To make the behavior of the VPN route advertisement deterministic, BGP would always prefer to advertise the locally generated route from the VRF source over that of the VPN route (route-reflector).		

Closed defects with code changes in R05.6.00e version 2

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00e. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID. This list was closed on January 20, 2015.

NOTE: This new report was generated on January 20, 2015. The only change was the listing of the following defects.

Defect ID: DEFECT000515839	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: BGP4 (IPv4)
Symptom: Inbound ACL is not working on VeoVPLS connection.	
Condition: When an inbound ACL is applied on an interface that is used as a VPLS endpoint, packets are not filtered.	

Defect ID: DEFECT000526237	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: Other IPv4
Symptom: Using the "show ip network" command after a VRRP failover, in some cases, the incorrect nexthop may be observed on a NetIron CER device.	
Condition: This issue is seen when VRRP failover occurs on devices connected to a NetIron CER, and the VIP MAC address is not shared between these devices.	

Closed defects with code changes in R05.6.00e

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00e. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID. This list was closed on December 5, 2014.

Defect ID: DEFECT000380652	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: IP Multicast
Reported In Release: NI 05.2.00	Technology Area: IPv4 Multicast Snooping
Symptom: Temporary loss of multicast traffic can be seen in IGMP snooping over VPLS when group membership changes	
Condition: In IGMP snooping over VPLS, when group membership changes temporary multicast traffic loss can be seen	

Defect ID: DEFECT000428705	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: IP Multicast
Reported In Release: NI 05.5.00	Technology Area: IPv4 Multicast Routing
Symptom: Router unexpectedly reloads on multicast task.	
Condition: Standby MP unexpectedly reloads on MCAST while adding lag port VLAN.	

Defect ID: DEFECT000462417	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.6.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Symptom: When doing an SNMPWalk some "bad i2c access (GIEI = set)" error messages are seen in the syslog when accessing the OID for power supply serial number.	
Condition: This is just a log message and has no impact on service.	

Defect ID: DEFECT000465350	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Traffic Management
Reported In Release: NI 05.6.00	Technology Area: Buffer Queue Management
Symptom: Traffic is dropping continuously in egress TM after reload.	
Condition: Traffic drops in Egress TM of 2x100g module when the DUT is reloaded with running traffic.	

Defect ID: DEFECT000475594	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.6.00	Technology Area: MRP - Metro Ring Protocol
Symptom: 100G ports show "Disabled" status instead of Forwarding/Blocking.	
Condition: MRP Port status gets disabled instead of forwarding or blocking.	

Defect ID: DEFECT000475897	
Technical Severity: High	Probability: Low
Product: Multi-Service IronWare	Technology: Monitoring/RAS
Reported In Release: NI 05.6.00	Technology Area: OAM - Operations, Admin & Maintenance
Symptom: System reports power supply issues after boot up.	
Condition: System reload and power supply I2C read failure messages are displayed on the telnet/console session.	

Defect ID: DEFECT000479068	
Technical Severity: High	
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: AAA
Symptom: A request for authentication, accounting or authorization fails unexpectedly. A "debug ip aaa" trace of the failure shows the following message among the debug output. <pre> xmr#Jan 10 11:00:17.392 =====AAA: Cleanup session 1 information. Jan 10 11:00:17.393 AAA authen response deferred - itc error (18) Jan 10 11:00:51.999 =====AAA: Cleanup session 11 information. Jan 10 11:00:52.000 AAA authen response deferred - itc error (18) </pre>	
Condition: When the CLI client times out prior to the timeout on waiting for a response from the AAA server approximately 110 thousand times it will result in a deferred response context handle being depleted completely due to a leak of the deferred response handles. This will prevent any further response being generated from the AAA engine.	
Workaround: - Avoid the number of AAA server (TACACS+,RADIUS) timeouts. - Do not let the telnet/ssh client time out before the AAA server times out.	
Recovery: If the console is available, allow access without AAA, then suspend authorization and accounting until an upgrade to a patched version of code can be loaded.	

Defect ID: DEFECT000482336	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: IP Multicast
Reported In Release: NI 05.4.00	Technology Area: IPv4 Multicast Routing
Symptom: Stale OIF entries seen in mcache entries which can lead to unnecessary forwarding of multicast traffic	
Condition: mcache entries with stale OIF entries that can result in unwanted forwarding of multicast traffic	

Defect ID: DEFECT000484932	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.7.00	Technology Area: Link Aggregation
Symptom: On deploying LAG with "tcp adjust-mss" configured on incoming interface, the line card reloads unexpectedly.	
Condition: LP unexpectedly reloads on deploying LAG with "tcp adjust-mss" configured on the port.	

Defect ID: DEFECT000488953	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: Static Routing (IPv4)
Symptom: When a static route is configured, the 'sh ip network' output does not show the configured next hop and instead shows the direct next hop.	
Condition: In some cases, an invalid IP address is displayed when the MAC address is 0. This is not service impacting.	

Defect ID: DEFECT000490442	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: OSPF (IPv4)
Symptom: OSPF Inter-area routes missing in the routing table.	
Condition: This issue happens when there are multiple OSPF neighbors on a broadcast interface in the backbone area. SPF for backbone area gets skipped in such a condition.	

Defect ID: DEFECT000490783	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: Licensing
Symptom: When the Management modules are upgraded to MR2, standby module unexpectedly reboots.	
Condition: The following conditions must apply: <ol style="list-style-type: none"> 1. More than 20 licenses are available in the system 2. Management module is upgraded to MR2 3. Applying a license while the system is not completely stable. 	
Workaround: Delete the license that causes the issue and reapply it when the system is stable.	

Defect ID: DEFECT000494399	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Symptom: Unexpected reload on execution of 'debug packet-buffer' LP CLI command with a BR-MLX-10Gx24-DM module.	
Condition: When the LP CLI command 'debug packet-buffer' is executed on a BR-MLX-10Gx24-DM module, the line card may unexpectedly reload.	

Defect ID: DEFECT000496594	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Traffic Management
Reported In Release: NI 05.7.00	Technology Area: Scheduling
Symptom: Traffic drops occur when traffic is running with port to port configurations at 100G line-rate (on MLX2x100G-X) with fixed 128B size packets.	
Condition: Must have line rate with fixed packet size of 128 Byte.	
Recovery: Reduce the traffic rate to match the expected throughput results.	

Defect ID: DEFECT000497688	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Symptom: The SNMP MIB object bgpPeerFsmEstablishedTime, which is used to get the Established time (Up time) of a BGP peer, will reset once every 50 days. This can result in different up time in the CLI vs SNMP.	
Condition: This issue is seen when the BGP peer is in the UP state for more than 50 days.	
Workaround: Use the SNMP MIB object bgp4V2PeerFsmEstablishedTime to see the correct up time of the BGP peer. This object is from an IETF draft BGPv4 MIB.	

Defect ID: DEFECT000498138	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: AAA
Symptom: Upon changing the username, the interface hangs and traffic does not flow in a NetIron MLX chassis.	
Condition: SNMS task holds CPU for longer time than anticipated to validate the new password against the available history of passwords.	
Workaround: Clear the old passwords to reduce the validation time and avoid the interface hang and traffic loss.	
Recovery: - Use "no enable strict-password-enforcement". - Delete the user, and then re-add the same user to modify the password.	

Defect ID: DEFECT000503378	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: OSPF (IPv4)
Symptom: When Type 7 and Type 5 routes are available, even when the cost associated with the Type 5 forwarding address is lower, the Type 7 route is selected.	
Condition: This occurs because of erroneous tie-breaker selection.	

Defect ID: DEFECT000504993	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Symptom: The mcache update causes BFD to drop session unexpectedly.	
Condition: On mcache update, BFD session flaps may be seen in GEN1 cards.	

Defect ID: DEFECT000506076	
Technical Severity: High	Probability: Low
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.7.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Symptom: Random high invalid counter values are received intermittently, when physical interface statistics (like ifDiscards and ifErrors) are fetched using SNMP get/getnext.	
Condition: SNMP Get on physical interface statistics (like ifErrors/Discards).	
Workaround: Disable the SNMP prefetch caching using the CLI command 'snmp-server cache disable'	

Defect ID: DEFECT000508412	
Technical Severity: Critical	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Symptom: Protocol session flaps may be seen along with CPU bound traffic loss.	
Condition: Data Path forwarding will not be affected.	

Defect ID: DEFECT000508833	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Symptom: An SFM link goes down immediately after BR-MLX-40Gx4-M is inserted.	
Condition: Problem showed up on multiple chassis multiple times.	

Defect ID: DEFECT000509112	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.2.00	Technology Area: ACLs (IPv4)
Symptom: Traffic is not forwarding outbound on 100G line card.	
Condition: This occurred when a 2x100 module was inserted into a slot that was previously configured for a 4x10 module.	

Defect ID: DEFECT000513916	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: System
Reported In Release: NI 05.4.00	Technology Area: Component
Symptom: Newly inserted hSFM in MLXe display incorrect up-time (355 days).	
Condition: Insert hSFM into MLXe.	

Defect ID: DEFECT000515245	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: System
Reported In Release: NI 05.4.00	Technology Area: CLI
Symptom: Retrieval of reset stack dump through “dm save” command may cause a system reset.	
Condition: Retrieval of reset stack dump through “dm save” command.	

Defect ID: DEFECT000515686	
Technical Severity: High	Probability: Low
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.6.00	Technology Area: MPLS Traffic Engineering
Symptom: If an MPLS configuration is highly scaled and the system is put under heavy stress through negative actions like frequent interface-flaps that are expected to alter the MPLS-TE database; and this is accompanied by the frequent execution of show commands to obtain detailed display of RSVP LSPs via a script, the system may unexpectedly reboot.	
Condition: MPLS is highly scaled with thousands of LSPs and interface flaps are frequent, accompanied by frequent execution of show commands to display detailed information for RSVP LSPs via a script.	

Defect ID: DEFECT000515781	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: BGP4 (IPv4)
Symptom: Unexpected reload of the management module may occur upon issuing the command 'no ip community-list extended TRANSIT-ANNOUNCE seq 5 permit <as-path>'	
Condition: After issuing a specific BGP CLI command.	

Defect ID: DEFECT000517133	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Symptom: All SFM links connected to the 2x100G-X line card (CFP-based) experience admin shutdown after the insertion of 2x100G line card.	
Condition: Insertion of 2x100G-X (CFP-based) line card on a chassis where at least one switchover of MP has occurred.	
Workaround: power-on all SFM links that are powered down by software.	

Defect ID: DEFECT000518360	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.6.00	Technology Area: Licensing
Symptom: After upgrading the version from 5.6.00b to 5.6.00c, "show version" displays that the BR-MLX-100Gx2-X has only 1 port license, MLXe_1PORT_100G.	
Condition: License for 100Gx2 installed.	

Defect ID: DEFECT000518532	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.4.00	Technology Area: MPLS VLL
Symptom: Service impact is seen during switchover from primary LSP to backup LSP.	
Condition: Switching over LSP from primary to secondary causes VLL traffic to drop.	

Defect ID: DEFECT000518919	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Monitoring/RAS
Reported In Release: NI 05.4.00	Technology Area: OAM - Operations, Admin & Maintenance
Symptom: 'show tm stat' indicates smaller counter value in comparison to a counter value of 'show np stat' and 'show interface' on 2x100G module.	
Condition: 'show tm stat' counter may indicate incorrect value	
Workaround: Run the "show tm stat" periodically	

Defect ID: DEFECT000520845	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.4.00	Technology Area: Topology Groups
Symptom: MLX may unexpectedly reload when performing the following sequence of steps: - Reload MLX, Power-off LPs, Remove Module, Remove RSTP,LAG and do not apply a module.	
Condition: Following the same steps, the issue is not reproduced.	

Defect ID: DEFECT000521851	
Technical Severity: High	Probability: Low
Product: Multi-Service IronWare	Technology: Traffic Management
Reported In Release: NI 05.6.00	Technology Area: Buffer Queue Management
Symptom: Traffic outage on newly inserted MLX24x10G line card, or line card replacement.	
Condition: Traffic outage on ports on 3rd tower of MLX24x10G line cards, and traffic outage when 1-tower or 2-tower line card is replaced with 2-tower or 3-tower line card respectively.	
Workaround: Reload chassis.	

Defect ID: DEFECT000526237	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: Other IPv4
Symptom: In some cases, incorrect nexthop may be observed on a NetIron CER device using "show ip network" command after a VRRP failover.	
Condition: Issue seen when VRRP failover is done on devices connected to NetIron CER and VIP MAC address is not shared between these devices.	

Defect ID: DEFECT000526276	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: ACLs (IPv4)
Symptom: DENY ACL applied on secondary LAG port causes packet drop on the primary LAG port.	
Condition: Configuring 'acl-frag-conservative' causes packet drops.	
Workaround: Not to use this option 'acl-frag-conservative', which can lead to unpredictable behavior.	

Defect ID: DEFECT000526352	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Symptom: Second generated TM log may overwrite the first generated TM log upon issuing command "clear tm log".	
Condition: When "clear tm log" is issued before TM events.	

Defect ID: DEFECT000526472	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.8.00	Technology Area: SSH - Secure Shell
Symptom: Vulnerability Summary for CVE-2008-5161: Overview Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.	
Condition: Fix required to address Vulnerability CVE-2008-5161:	

Defect ID: DEFECT000526713	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: IP Multicast
Reported In Release: NI 05.6.00	Technology Area: IPv4 Multicast Snooping
Symptom: IGMP query may be sent out from a port without multicast snooping enabled before the port transitions to RSTP forwarding state.	
Condition: When RSTP is enabled and multicast snooping is not enabled on the VLAN.	

Defect ID: DEFECT000528112	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: BGP4 (IPv4)
Symptom: After a BGP peer having the shortest AS-path flaps, the path is not selected as the best path again.	
Condition: When the neighbor with shortest AS PATH flaps.	
Workaround: Clearing BGP neighbor	

Defect ID: DEFECT000528121	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.6.00	Technology Area: IEEE 802.1d STP
Symptom: "No span" configuration may not appear under secondary ports of the LAG after the LAG is undeployed.	
Condition: Undeploying a LAG with "no span" configured on the primary port of the LAG.	

Defect ID: DEFECT000528476	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.4.00	Technology Area: LDP
Symptom: NetIron device may reset unexpectedly upon executing command "no router mpls" in LDP over GRE topology.	
Condition: Executing command "no router mpls" in LDP over GRE topology.	

Defect ID: DEFECT000528511	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.6.00	Technology Area: VPLS - Virtual Private LAN Services
Symptom: Convergence time takes more than 50ms in the range of 200-300msec.	
Condition: When FRR and VLL are both involved, convergence will take longer time interval.	

Defect ID: DEFECT000529076	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.8.00	Technology Area: VPLS - Virtual Private LAN Services
Symptom: For the network built with ISIS-TE policy in MPLS and using RSVP defined path with LSP, standby path and FRR, it is observed that on the first fiber cut either after a reboot of the router or after waiting X hours, the convergence time is around 200ms. Subsequent fiber cuts and restores are under 10ms.	
Condition: VPLS MAC entries are getting flushed inadvertently under MPLS FRR with RSVP-TE VPLS failover scenario causing high convergence time which results in traffic loss for more time.	

Defect ID: DEFECT000530014	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Monitoring/RAS
Reported In Release: NI 05.5.00	Technology Area: OAM - Operations, Admin & Maintenance
Symptom: Seeing issues with CFM DMM not working when two DMM sessions are initiated simultaneously.	
Condition: Issue simultaneous DMM sessions, which will result in failure.	

Defect ID: DEFECT000530066	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: System
Reported In Release: NI 05.4.00	Technology Area: CLI
Symptom: Occasionally, upon entering the configuration mode on a NetIron MLX device, user may unexpectedly observe "Warning: 1 users (s) already in config mode" message when no other user is logged into the device.	
Condition: See customer symptom.	

Defect ID: DEFECT000532927	
Technical Severity: Critical	Probability: High
Product: Multi-Service IronWare	Technology: Security
Reported In Release: NI 05.8.00	Technology Area: Security Vulnerability
Symptom: The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC mode ciphers. This affects most current browsers and websites, but also includes any software that either references a vulnerable SSL/TLS library (e.g. OpenSSL) or implements the SSL/TLS protocol suite itself.	
Condition: Disable the support for SSL 3.0 due to protocol vulnerability.	

Defect ID: DEFECT000534024	
Technical Severity: Critical	Probability: Medium
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.6.00	Technology Area: VPLS - Virtual Private LAN Services
Symptom: On executing "disable" command in the interface, the device unexpectedly reloads and LP may throw an EXCEPTION.	
Condition: Device unexpectedly reloads on executing interface "disable".	

Defect ID: DEFECT000535095	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: OSPF (IPv4)
Symptom: ECMP routes are not displayed correctly in 'show ip routes'	
Condition: MLX not considering equal cost paths for external LSA type	

Defect ID: DEFECT000536035	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.8.00	Technology Area: MPLS Traffic Engineering
Symptom: MLX MP may unexpectedly switchover to standby MP while upgrading to a new image	
Condition: When upgrading to a new image, MLX MP may unexpectedly reload and cause a switchover to the standby MP	

Defect ID: DEFECT000536537	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: System
Reported In Release: NI 05.4.00	Technology Area: CLI
Symptom: "Unrecognized command" message is displayed when attempting to configure "confirm-port-down" on a 10G interface.	
Condition: One of the slots has a 10G XFP inserted while the interface is in link up state with traffic. The other slot is empty. The interface setting "confirm-port-down" configured under the interface in use should allow a user to insert an XFP into the empty slot without flapping the in-use interface.	

Closed defects with code changes in R05.6.00d

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00d. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID. This list was closed on August 7, 2014.

Defect ID:	DEFECT000454591		
Technical Severity:	High	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	OSPF (IPv4)
Symptom:	OSPF flaps.		
Condition:	OSPF session resets due to too many retransmissions.		

Defect ID:	DEFECT000457684		
Technical Severity:	Medium	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	CES/CER fails to update the Next Hop Table with the Gratuitous ARP, resulting in reachability issues.		
Condition:	Redundant network interfaces failing over between two CES/CERs wherein the Gratuitous ARP generated by the failed over node is not considered for Next Hop Table update.		

Defect ID:	DEFECT000471046		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.6.00	Technology Area:	Multi-Chassis Trunking
Symptom:	With large number of MCT clients, the reload results in some clients FSM state to be in Local Up/Remote Up.		
Condition:	With large number of MCT clients, the reload results in some clients FSM state to be in Local Up/Remote Up.		

Defect ID:	DEFECT000473619		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	OSPFv3 (IPv6)
Symptom:	OSPFv3 "max metric" is not generated when "wait for bgp" is configured and OSPF router ID is not configured explicitly		
Condition:	1) OSPFv3 configured with "wait for bgp" 2) OSPFv3 router ID is not set explicitly		

Defect ID:	DEFECT000474815		
Technical Severity:	Medium	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.6.00	Technology Area:	BFD - BiDirectional Forwarding Detection
Symptom:	BFD timer value for 150ms flaps when system max mac value is configured for 2097152.		
Condition:	With this max mac config, Min time will always be around ~158 ms. Since the Time-sensitive protocol is less than 155ms, the flap occurs.		

Defect ID:	DEFECT000475432		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.4.00	Technology Area:	SNMPv2, SNMPv3 & MIBs
Symptom:	The incorrect value will be displayed in TRAP message.		
Condition:	On any notification through TRAP, incorrect slot value will be displayed in the TRAP message.		

Defect ID:	DEFECT000478534		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	The 'Show Optic' output for 100G-CFP-ER4 incorrectly shows 15 lanes.		
Condition:	'Show Optic' output for 100G-CFP-ER4 incorrectly shows 15 lanes.		

Defect ID:	DEFECT000482336		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	The OIF timer memory pool became exhausted on the distribution switch.		
Condition:	Potentially, this can lead to stale OIFs that never age out..		

Defect ID:	DEFECT000484791		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.4.00	Technology Area:	AAA
Symptom:	Users with non-zero privilege are deleted after a reload.		
Condition:	<ol style="list-style-type: none"> 1. Configure super user1 with priv 0 2. Configure user1 with priv 4 3. Configure user2 with priv 5 4. Configure super user2 with priv 0 5. Delete super user1, save user Config and reload 6. user1, user2 are additionally removed on reload 		
Workaround:	Avoid deletion of super user displayed first in the 'show users' command output.		
Recovery:	To delete the first super user X: <ol style="list-style-type: none"> 1. Add super user account Y, save user config and log out 2. Log in using super user account Y 3. Delete the super user account X 4. Add super user account Z to avoid deletion of other users 		

Defect ID:	DEFECT000485529		
Technical Severity:	Low	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.7.00	Technology Area:	OSPF (IPv4)
Symptom:	The 'Show ip ospf interface ve ' output is printed multiple times for some interfaces.		
Condition:	MCT is configured with VEOVPLS and OSPF enabled.		

Defect ID:	DEFECT000487660		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.3.00	Technology Area:	VLAN
Symptom:	A provider-network port cannot be added as untagged member of a VLAN.		
Condition:	If CDP or FDP is enabled, a provider network port is made untagged member of the Control VLAN, so it cannot be made untagged member of an SVLAN.		

Defect ID:	DEFECT000489647		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	Prefix Lists (IPv4)
Symptom:	Line card may unexpectedly reset when there is host traffic, and when the host sending the traffic exists on VPLS remote endpoint.		
Condition:	Host traffic from a host learned on VPLS VE remote endpoint.		

Defect ID:	DEFECT000494107		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Certain flows are not being programmed correctly on an XMR.		
Condition:	During system reload, the nexthop interface UP event arrived later than the nexthop entry and ARP entry downloaded to the LP, which caused the nexthop entry to get stuck and never come up.		

Defect ID:	DEFECT000496155		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.3.00	Technology Area:	Other
Symptom:	Line card Image not getting loaded on inserting modules		
Condition:	When there is no line cards inserted in a chassis and if they are inserted after switchover, then the line cards are not booting up.		
Recovery:	Reloading the chassis will help in recovery.		

Defect ID:	DEFECT000498016		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	ACLs (IPv4)
Symptom:	When the running configuration of the router the ACL configurations (L2, IPv4, IPv6) might not be synchronized correctly.		
Condition:	When the configuration is modified through TFTP/SCP while the MP is syncing the configurations to LPs & standby, the ACL configurations might not sync correctly.		

Defect ID:	DEFECT000498180		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Traffic Management
Reported In Release:	NI 05.6.00	Technology Area:	QoS - Quality of Service
Symptom:	The command 'sh qos-map dscp encode/decode-map' is not displaying the expected output.		
Condition:	The command 'sh qos-map dscp encode/decode-map' is not displaying user configured encode/decode map names.		

Defect ID:	DEFECT000499368		
Technical Severity:	Low	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	PSU flap SYSLOG message and PSU shutdown.		
Condition:	Input power source flap leading to PSU flap SYSLOG message and PSU shutdown.		
Recovery:	Provide stable input power source to PSU units and power on PSU manually.		

Defect ID:	DEFECT000500043		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	In CES/CER, when giant frames are received they are updated in the ignored frame count rather than the giant frame count of interface statistics. Other interface statistics like input errors, CRC errors, runs, and giants are displayed as zero.		
Condition:	Consult the Configuration Guide for usage of "show statistics ethernet <slot/port>" on receiving giant packets on interface.		

Defect ID:	DEFECT000500944		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.5.00	Technology Area:	IS-IS (IPv6)
Symptom:	MP IPv6 application (e.g., Ping) not sending packet on the correct interface or the result of 'Show ipv6 cache <address> out interface' is not same as 'show ipv6 route <ipv6 address> out-interface'.		
Condition:	If a route is replaced by the same type of route but the interface is different, the IPv6 route cache port is not updated.		
Recovery:	'Clear IPv6 cache <ipv6-address>' will resolve this issue.		

Defect ID:	DEFECT000501070		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	Interface setting 'confirm-port-up' should have a configurable range of 0 to 100, but with a value of 32 or higher, the running config displays the remainder of dividing the entered value by 32.		
Condition:	Adding a value of 32 or higher to an interface config with "confirm-port-up", the value in the running config will be the remainder of dividing the entered value by 32.		

Defect ID:	DEFECT000501101		
Technical Severity:	Low	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	The interface configuration 'confirm-port-up <count>' gets removed with invalid port up count in 'no confirm-port-up <count>'.		
Condition:	Invalid port up count usage in 'no confirm-port-up <count>'.		

Defect ID:	DEFECT000501252		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Security
Reported In Release:	NI 05.6.00	Technology Area:	FIPS
Symptom:	While setting up a secure TLS connection to the audit server, the remote TLS server certificate is not being authenticated by the local TLS client. This is a requirement for Common Criteria certification. Affected releases: NI 5.3, 5.5 and 5.6.		
Condition:	This is a Request For Enhancement (RFE) resulting from Common Criteria Certification requirements, mandating that the certificate presented by the audit server for the TLS connection be validated.		

Defect ID:	DEFECT000501365		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.7.00	Technology Area:	SNMPv2, SNMPv3 & MIBs
Symptom:	SNMP request times out consistently while polling ifTable and ifXTable.		
Condition:	Issue is seen when a lag's member port spans across multiple modules. If user polls IfTable/IfTable for such a lag, it may result in the SNMP request getting timed out.		

Defect ID:	DEFECT000501705		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	Packets with maximum MTU size may be dropped in hardware for a VE interface.		
Condition:	Interface MTU configuration present on a VE interface.		
Workaround:	Set interface MTU to be four bytes greater than that of the neighboring node.		

Defect ID:	DEFECT000501841		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	BGP4+ (IPv6)
Symptom:	When an IPv6 BGP peer is configured and added to a peer-group at the default BGP configuration mode (config-bgp), IPv6 unicast is not enabled for the peer, even if the peer-group is enabled for IPv6 unicast. As a result, IPv6 BGP routes are not advertised to the peer.		
Condition:	This happens if an IPv6 BGP peer is configured or added in the default BGP mode.		
Workaround:	Configure the IPv6 BGP peer at the 'address-family ipv6 unicast' mode, or activate the IPv6 BGP peer explicitly in 'address-family ipv6 unicast' mode.		

Defect ID:	DEFECT000502907		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	IP Multicast
Reported In Release:	NI 05.4.00	Technology Area:	IPv4 Multicast Routing
Symptom:	Simultaneous unexpected reset on two MLX routers.		
Condition:	Mtrace response handler may cause a reset on an MLX router in certain scenarios.		

Defect ID:	DEFECT000503134		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.7.00	Technology Area:	VLAN
Symptom:	Ports in the VLAN are in the DISABLED state, and many ITC errors appear upon the reload of the router.		
Condition:	Issues occur during reload of the router.		

Defect ID:	DEFECT000503181		
Technical Severity:	Critical	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Monitoring/RAS
Reported In Release:	NI 05.6.00	Technology Area:	OAM - Operations, Admin & Maintenance
Symptom:	When 'ctrl-c' is executed on an interface module before 'show cpu histogram sequence' has completed execution, the interface module may unexpectedly reload.		
Condition:	Service on the ports on the affected interface module will be impacted for ~1 minute while the module reloads.		

Defect ID:	DEFECT000503352		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.5.00	Technology Area:	ACLs (IPv4)
Symptom:	Outbound ACL is not hitting for software forwarded L3 packets when inbound ACL is hit.		
Condition:	Set the TXA bit in forwarding path to hit outbound ACL.		

Defect ID:	DEFECT000503378		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	OSPF (IPv4)
Symptom:	When Type 7 and Type 5 routes are available, even when the cost associated with the Type 5 forwarding address is lower, the Type 7 route is selected.		
Condition:	This occurs because of erroneous tie-breaker selection.		

Defect ID:	DEFECT000503443		
Technical Severity:	Medium	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Monitoring/RAS
Reported In Release:	NI 05.6.00	Technology Area:	SYSMON
Symptom:	A number of irrelevant and non-impacting AgeRAM errors appear in the Syslog.		
Condition:	This behavior was introduced in 5.6.00 code, which applied additional monitoring capabilities.		

Defect ID:	DEFECT000503805		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Traffic Management
Reported In Release:	NI 05.7.00	Technology Area:	QoS - Quality of Service
Symptom:	System with OpenFlow interfaces is running an overnight script that includes disabling/enabling OF ports and bringing LPs up/down. After a few iterations, two LPs: MLX24x10G and MLX2x100-CFP unexpectedly reset with reason code "20" and messages about "FE600_SRD_EPB_ACCESS_ERR"		
Condition:	The issue is related to link power up based on remote LP bootup. It was introduced since the autonomous link power down was introduced when a LP is not available or down to avoid cross talks by un-terminated links.		
Workaround:	This feature is itself a recovery mechanism. To disable this feature configure as: system-init fe-access-recovery-disable.		

Defect ID:	DEFECT000503931		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	On 8x10G card, the all ports are in up state but unresponsive.		
Condition:	The ports in 8x10G line card are in UP state, but not reachable and traffic is dropped.		
Recovery:	Power cycle the affect 8x10G line card		

Defect ID:	DEFECT000504265		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Running 'show chassis' command displays an invalid module with power usage 640W in slot 7, which is an empty slot.		
Condition:	See customer symptom		
Recovery:	Insert a module in the slot that will not be able to boot (wrong software version) and then remove it.		

Defect ID:	DEFECT000504333		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Software forwarding of packets from regular interface to VPLS-VE interface will be dropped. In CER, Software forwarding happens for all control packets which are trapped to CPU and the first packet for directly connected interface.		
Condition:	If the Rx packets from the L3 interface (phy/ve) are trapped to the CPU for software forwarding; and if the outgoing interface is a VPLS-VE interface, these packets will be dropped.		

Defect ID:	DEFECT000504992		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	IP Multicast
Reported In Release:	NI 05.4.00	Technology Area:	IPv4 Multicast Routing
Symptom:	High CPU usage on downstream multicast router due to erroneous upstream OIF forwarding.		
Condition:	See customer symptom.		

Defect ID:	DEFECT000504993		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Mcache update causes BFD to drop session unexpectedly.		
Condition:	See customer symptom.		

Defect ID:	DEFECT000506652		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.6.00	Technology Area:	ACLs (IPv6)
Symptom:	A response is generated for incoming IPv6 anycast packets, showing that a Receive ACL is not filtering properly.		
Condition:	The filter is not working properly and placing a higher demand than normal on the CPU.		

Defect ID:	DEFECT000506837		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	SDN
Reported In Release:	NI 05.6.00	Technology Area:	OpenFlow 1.0
Symptom:	When the MLXe-16 is disconnected / reconnected to the openflow controller, packets traversing the MLXe-16 are dropped by the default drop rule.		
Condition:	See customer symptom		

Defect ID:	DEFECT000507001		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Packets might not be routed between regular VE and VPLS-VE		
Condition:	Src port and Dst Port is the same phy port, Src interface is VE and dst interface is VPLS-VE.		
Workaround:	Brocade(config)# no ip icmp redirects		

Defect ID:	DEFECT000507654		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.4.00	Technology Area:	VSRP - Virtual Switch Redundancy Protocol
Symptom:	VSRP temporarily transitions to Master-Master state due to a delay in the generation of "Hello's" from the VSRP Master node. This can cause duplicate IP address messages to be seen on both the nodes for the VSRP Virtual IP.		
Condition:	Transient VSRP Master-Master scenario along with duplicate IP messages for the VSRP VIP on the VSRP nodes		
Workaround:	Increase the VSRP "Hello" timer appropriately.		

Defect ID:	DEFECT000508168		
Technical Severity:	Low	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Monitoring/RAS
Reported In Release:	NI 05.6.00	Technology Area:	Syslog
Symptom:	Configurable option for Syslog is missing.		
Condition:	Lack of support for syslog action for sysmon tm ingress-dram-crc command.		

Defect ID:	DEFECT000508381		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	When applying or modifying flow control, unable to reset flow control configuration to default.		
Condition:	Disable of interface flow control was not applied to the traffic		

Defect ID:	DEFECT000508412		
Technical Severity:	Critical	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	OSPF goes to Init state and Traffic loss occurs.		
Condition:	See customer symptom		

Defect ID:	DEFECT000508833		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	An SFM link goes down immediately after BR-MLX-40Gx4-M gets inserted.		
Condition:	See customer symptom.		

Defect ID:	DEFECT000509112		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.2.00	Technology Area:	ACLs (IPv4)
Symptom:	Traffic is not forwarding outbound on 100G line card.		
Condition:	This occurred when a 2x100 module was inserted into a slot that was previously configured for a 4x10 module.		

Defect ID:	DEFECT000510095		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.6.00	Technology Area:	SSH - Secure Shell
Symptom:	User may notice memory depletion on the management module after SSH access into the router.		
Condition:	The cipher context used by SSH protocol is not freed after its use.		
Workaround:	Use TELNET or Console instead of SSH to access the device.		

Defect ID:	DEFECT000510188		
Technical Severity:	Critical	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.7.00	Technology Area:	Multi-VRF (IPv6)
Symptom:	Management interface is not reachable when IPv6 address is configured		
Condition:	See customer symptom		

Defect ID:	DEFECT000510632		
Technical Severity:	Critical	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	SDN
Reported In Release:	NI 05.6.00	Technology Area:	OpenFlow 1.0
Symptom:	Router unexpectedly resets when 'opm_handle_flow_stat_req' is run with task 'openflow_opm'.		
Condition:	The problem occurs when modification and query flow stats are performed at the same time.		

Defect ID:	DEFECT000512023		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.4.00	Technology Area:	VPLS - Virtual Private LAN Services
Symptom:	MP and LP remaining out of synch for some VPLS MACs. This results in high CPU condition on LP as packets destined to those addresses are treated as unknown unicasts and hence get SW forwarded		
Condition:	Large number of VPLS endpoints some of which contain LAG based endpoints spanning multiple LP slots		

Defect ID:	DEFECT000512044		
Technical Severity:	Critical	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	In certain cases Module may reset while executing 'dmsg' command from LP OS.		
Condition:	See customer symptom		

Defect ID:	DEFECT000512232		
Technical Severity:	High	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.5.00	Technology Area:	OSPF (IPv4)
Symptom:	NI OSPF router fails to establish a neighbor session, or receive routes from a neighbor.		
Condition:	This condition happens when an OSPF router in the network has more than 672 IP interface addresses.		
Workaround:	Limit the number of IP addresses configured on a router to no more than 672.		

Defect ID:	DEFECT000512234		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.6.00	Technology Area:	SNMPv2, SNMPv3 & MIBs
Symptom:	If a SNMP GET or GETNEXT is performed on a non-existent VRF using an invalid index for the bgp4V2NlriTable, the device would unexpectedly reload.		
Condition:	See customer symptom		

Defect ID:	DEFECT000512560		
Technical Severity:	Critical	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Security
Reported In Release:	NI 05.7.00	Technology Area:	Receive ACLs
Symptom:	User can see an unexpected reset of the telnet task when the command 'show access-list receive accounting brief' fails to retrieve data from LP.		
Condition:	See customer symptom		

Defect ID:	DEFECT000513517		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.6.00	Technology Area:	DNS (IPv6)
Symptom:	IPv6 DNS resolution in traceroute is not working		
Condition:	See customer symptom.		

Defect ID:	DEFECT000513554		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.2.00	Technology Area:	IP over MPLS
Symptom:	Device may unexpectedly reload when processing ICMP trace route response that includes MPLS extension object.		
Condition:	Issuing a ICMP trace route to a destination that might include MPLS tunnels in its path.		

Defect ID:	DEFECT000513905		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	SDN
Reported In Release:	NI 05.6.00	Technology Area:	OpenFlow 1.0
Symptom:	Issue in changing the OpenFlow interface mode from layer 2 to layer 3.		
Condition:	See customer symptom.		

Defect ID:	DEFECT000514273		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	On SNMPWALK, a nonexistent module is displayed.		
Condition:	For an empty slot, SNMPWALK reports a module is present.		
Workaround:	Remove the module from the chassis and delete the module using the "no module" CLI command.		

Defect ID:	DEFECT000514437		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.6.00	Technology Area:	Other
Symptom:	Creation of unexpected pending ARP entries for remote destinations and high CPU condition in MP		
Condition:	High number of TTL expiry and sFlow packets in the system along with pending ARP entries created even for the associated remote destinations. High CPU condition on MP due to large number of ARP requests being generated		

Defect ID:	DEFECT000514593		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	OSPF (IPv4)
Symptom:	Traffic is lost when the LSP changes due to an auto bandwidth adjustment for next hops learned over the MPLS uplink in the VEOVPLS setup.		
Condition:	The issue happens when the auto bandwidth adjustment is enabled for LSPs. The adjustments resulted in creating a new LSP with a new label, but the new label did not get updated in the forwarding database of the packet processor.		

Defect ID:	DEFECT000514641		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Unable to load startup configuration.		
Condition:	This occurs when there are more than 2048 characters within the startup configuration of VLAN 1.		
Workaround:	Download the startup configuration and remove the 'no-dual' configuration; then download the startup config before reloading the box.		

Defect ID:	DEFECT000514654		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Other
Reported In Release:	NI 05.4.00	Technology Area:	Other
Symptom:	Executing 'config t' causes VRRP to flap.		
Condition:	This will usually occur on a reload, when 'no dual-mode-default-vlan' is configured and all of the available ports of the MLX32 are configured as tagged.		
Workaround:	TFTP or SCP download the startup configuration and remove the 'no-dual-default-vlan' configuration; and copy back the modified startup config before reloading the box.		

Defect ID:	DEFECT000514900		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.4.00	Technology Area:	SNMPv2, SNMPv3 & MIBs
Symptom:	Device gets reloaded unexpectedly with stack trace.		
Condition:	See customer symptom.		

Defect ID:	DEFECT000514917		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	Management
Reported In Release:	NI 05.6.00	Technology Area:	SNMPv2, SNMPv3 & MIBs
Symptom:	If there exists an OSPF area with area-id 255.255.255.255 in the configuration, then the SNMP walk on the table ospfAreaTable will go into a loop. SNMP managers like net-snmp will detect this and report a lexicographic error on this table.		
Condition:	When an OSPF area with area-id 255.255.255.255 is configured in the system and a SNMP walk/get-next operation is executed on the ospfAreaTable.		
Workaround:	<p>1) Avoid doing a SNMP walk on ospfAreaTable when there is an area with area-id 255.255.255.255 in the system. Use the CLI commands to read the area related information.</p> <p>2) Another option is to avoid configuring an OSPF area with area-id 255.255.255.255. This will not cause any issue with the SNMP walk operations for the ospfAreaTable.</p>		

Defect ID:	DEFECT000515280		
Technical Severity:	High	Probability:	High
Product:	Multi-Service IronWare	Technology:	IP Multicast
Reported In Release:	NI 05.5.00	Technology Area:	IPv4 Multicast Routing
Symptom:	When IGMP packets are received with a version different than the configured version, memory is not freed.		
Condition:	This issue occurs only when the system receives IGMP packets with a different version than what is configured.		

Defect ID:	DEFECT000515686		
Technical Severity:	High	Probability:	Low
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.6.00	Technology Area:	MPLS Traffic Engineering
Symptom:	If an MPLS configuration is highly scaled and the system is put under heavy stress through negative actions like frequent interface-flaps that are expected to alter the MPLS-TE database; and this is accompanied by the frequent execution of show commands to obtain detailed display of RSVP LSPs via a script, the system may unexpectedly reboot.		
Condition:	MPLS is highly scaled with thousands of LSPs and interface flaps are frequent, accompanied by frequent execution of show commands to display detailed information for RSVP LSPs via a script.		

Defect ID:	DEFECT000515781		
Technical Severity:	Medium	Probability:	Low
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.4.00	Technology Area:	BGP4 (IPv4)
Symptom:	Spontaneous MLXe4 reload after 'no ip community-list extended TRANSIT-ANNOUNCE seq 5 permit 49544:300'		
Condition:	See customer symptom		

Defect ID:	DEFECT000516576		
Technical Severity:	Medium	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.2.00	Technology Area:	OSPF (IPv4)
Symptom:	Management module may unexpectedly reload when attempting to configure 128th IP address for an interface.		
Condition:	When configuring 128th IP address, management module may unexpectedly reload.		
Workaround:	Avoid configuring 128th IP address for an interface.		

Defect ID:	DEFECT000517519		
Technical Severity:	Critical	Probability:	High
Product:	Multi-Service IronWare	Technology:	MPLS
Reported In Release:	NI 05.6.00	Technology Area:	VPLS - Virtual Private LAN Services
Symptom:	Active MP unexpectedly reloads after shutting down client-interfaces.		
Condition:	CT node (MCT2) reflects active MP issue at l2vpn task after executing client-interfaces shutdown.		
Workaround:	Execute "client-interface shutdown" on MCT VPLS/VLL Active MP.		

Defect ID:	DEFECT000517892		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 2
Reported In Release:	NI 05.6.00	Technology Area:	MAC ACLs
Symptom:	In a configuration where there are several IPv4 extended ACL's with different VLAN's as part of the TCP filters, removing one Filter is removing another ACL filter.		
Condition:	It occurs only when there is a VLAN clause added as part of the filter, specific to TCP.		

Defect ID:	DEFECT000517896		
Technical Severity:	Medium	Probability:	High
Product:	Multi-Service IronWare	Technology:	Layer 3
Reported In Release:	NI 05.2.00	Technology Area:	BGP4 (IPv4)
Symptom:	When removing or un-configuring a module that has BGP update-source configured on one of its interfaces, the BGP running configuration is corrupted.		
Condition:	BGP running configuration will be corrupted when removing or un-configuring a module that has BGP update-source configured on one of its interfaces.		
Workaround:	Un-configure and re-configure the affected BGP neighbor configuration.		

Defect ID:	DEFECT000521040		
Technical Severity:	High	Probability:	Medium
Product:	Multi-Service IronWare	Technology:	SDN
Reported In Release:	NI 05.6.00	Technology Area:	OpenFlow 1.0
Symptom:	IPv4 packets with TTL=1 in layer 2/3 hybrid mode on an OpenFlow enabled switch are dropped instead of being switched.		
Condition:	An IPv4 BGP session is not being established, but an IPv6 BGP session is. A ping with IPv4 packet ttl > 1 works fine, but same with ttl=1 results in dropped IPv4 packets.		

Closed defects with code changes in R05.6.00c

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00c. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID. This list was closed on April, 17, 2014.

Defect ID: DEFECT000435989	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.5.00	Technology Area: Multi-Chassis Trunking
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: CCEP ports may be in disabled state after MP switchover.	
Condition: This issue is observed in a scaled MCT setup, where the CCEP ports are in a disabled state.	
Recovery: Enable the disabled ports.	

Defect ID: DEFECT000471322	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.0.00	Technology Area: Topology Groups
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: The topology group does not show all the member VLANs added.	
Condition: When the number of VLANs added requires more printing space than was pre allocated, it will not display the extra VLANs added.	

Defect ID: DEFECT000476472	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.5.00	Technology Area: OSPF (IPv4)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: OSPF is retaining a stale route (more specific route) when connected routes are redistributed and there is a change in the interface address (/24 to /23 IP) that has been redistributed.	
Condition: This issue happens when a route redistributed to OSPF is being replaced by a supernet of the route for the same prefix.	

Defect ID: DEFECT000479068	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: AAA
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: A request for authentication, accounting or authorization fails unexpectedly. A "debug ip aaa" trace of the failure shows the following message among the debug output. <pre>xmr#Jan 10 11:00:17.392 ====AAA: Cleanup session 1 information. Jan 10 11:00:17.393 AAA authen response deferred - itc error (18) Jan 10 11:00:51.999 ====AAA: Cleanup session 11 information. Jan 10 11:00:52.000 AAA authen response deferred - itc error (18)</pre>	
Condition: When the CLI client times out prior to the timeout on waiting for a response from the AAA server approximately 110 thousand times it will result in a deferred response context handle being depleted completely due to a leak of the deferred response handles. This will prevent any further response being generated from the AAA engine.	
Workaround: - Avoid the number of AAA server (TACACS+,RADIUS) timeouts. - Do not let the telnet/ssh client time out before the AAA server times out.	
Recovery: If the console is available, allow access without AAA, then suspend authorization and accounting until an upgrade to a patched version of code can be loaded.	

Defect ID: DEFECT000479829	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: MPLS
Reported In Release: NI 05.2.00	Technology Area: LDP
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: When a line-card is malfunctioning it is possible that some of the entries for interfaces get duplicated in 'show mpls config'.	
Condition: The issue appears only when a line-card is malfunctioning. It is a display issue and does not cause any functional problems.	

Defect ID: DEFECT000483453	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: IP Multicast
Reported In Release: NI 05.4.00	Technology Area: IPv6 Multicast Routing
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Network is affected by constant multicast flooding, when MLXe sends 2 min of continuous ICMPv6-ND packets when trying to resolve non existing IPv6 hosts.	
Condition: When forwarding IPv6 packet for a node on a directly connected network ND6 resolution is performed by sending ND6 NS packet for the destination IPv6 address and if no ND6 NA response is received for some reason then attempt is made to resolve the address for 2 mins or until the response is received.	
Recovery: Use 'clear ipv6 cache <x:x::x:x>' command on LP to remove the cache entry for the host whose IPv6 address to MAC address cannot be resolved within few seconds.	

Defect ID: DEFECT000486553	
Technical Severity: Medium	
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Ports get disabled when configured with strict mode loop detection even though the interface has not received its own loop detect PDUs.	
Condition: This scenario will occur if the strict mode loop detect is configured.	
Workaround: Remove the strict mode loop detect configuration.	
Recovery: Remove the strict mode configuration and enable the ports manually.	

Defect ID: DEFECT000487033	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.4.00	Technology Area: Multi-Chassis Trunking
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Intermittent packet loss when pinging IPV6 host in MCT setup.	
Condition: The symptom will be observed when CCEP port goes down and the new path is via ICL port.	

Defect ID: DEFECT000487545	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: VRRP & VRRP-E (IPv4)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: With MCT VRRP-e PIM-SM being configured and VRRP-E short path forwarding feature enabled, when the VRRP-e Virtual IP is configured as the static Rendezvous Point (RP), duplicate IP address warnings are seen in the Syslog. Sample message - "Duplicate IP address xxx.xxx.xxx.x detected sent from MAC address yyyy.yyyy.yyyy interface a/b, n packets". This configuration is not supported.	
Condition: This issue is seen when attempting to use VRRP-e Virtual IP as the multicast static Rendezvous Point (RP) in an MCT VRRP-e setup with PIM-SM configured. This is not a supported configuration.	
Workaround: Do not use the VRRP-e Virtual IP as the static multicast RP.	
Recovery: Remove the unsupported configuration.	

Defect ID: DEFECT000487754	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: 24x10G line cards fabric links stay down during boot up.	
Condition: When a system with a mix of Gen1 and 24x10G cards that have FEC mode enabled is reloaded, the Gen1 line cards come up before the 24x10G line cards.	
Workaround: Bring up 24x10G cards before the Gen1 cards.	
Recovery: Power-off all the line cards. Bring up the 24x10G line cards first and then the Gen 1 line cards	

Defect ID: DEFECT000488018	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: CER 2024 unexpectedly reloaded.	
Condition: If the user executes hidden debug commands with a large number of routes, the router may unexpectedly reload.	

Defect ID: DEFECT000488216	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.4.00	Technology Area: VLAN
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Multiple interface modules may unexpectedly reload in an MLX chassis when trying to remove a port from the default VLAN membership.	
Condition: If an unsupported module is configured in the CLI and not present in the slot, when trying to remove a port on the slot (non-existing) from the default VLAN membership, it may cause multiple modules to unexpectedly reload.	
Workaround: Do not configure the module type "ni-xmr-20-port-1g".	

Defect ID: DEFECT000488422	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.2.00	Technology Area: VRRP & VRRP-E (IPv6)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: A router either rejects all incoming IPv6 VRRP hello packets for bad checksum, or the router's VRRP partner will reject all of the routers IPv6 VRRP hello packets.	
Condition: The issue only occurs if IPv6 VRRP is enabled and IPv4 VRRP is disabled.	
Workaround: This issue can be avoided by enabling IPv4 VRRP alongside IPv6 VRRP.	

Defect ID: DEFECT000488953	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: Static Routing (IPv4)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: When a static route is configured, the 'sh ip network' output does not show the configured next hop and instead shows the direct next hop.	
Condition: In some cases, an invalid IP address is displayed when the MAC address is 0. This is not service impacting.	

Defect ID: DEFECT000490442	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: OSPF (IPv4)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: OSPF Inter-area routes missing in the routing table.	
Condition: This issue happens when there are multiple OSPF neighbors on a broadcast interface in the backbone area. SPF for backbone area gets skipped in such a condition.	

Defect ID: DEFECT000490504	
Technical Severity: Medium	
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.3.00	Technology Area: MRP - Metro Ring Protocol
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Packet loop and high CPU were seen, when "forward-lacp" and "forward-lldp" are configured on MLX to establish LACP trunk over MRP.	
Condition: When forward LACP is enabled and there is any protocol blocking port on the node, the LACP BPDUs are not dropped, resulting in a loop condition.	
Recovery: Disable the blocking port to recover from the loop.	

Defect ID: DEFECT000490598	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: Telemetry
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: All line card modules and standby module unexpectedly reload with CARD_DOWN_REASON_LOSS_HEARTBEAT message.	
Condition: The configuration file that was applied, modifies the PBR configuration while still bound to interfaces.	
Recovery: - Unconfigure all PBR bindings from the interfaces. - Modify ACLs, route-maps, VLANs. - Apply back the PBR bindings to the interfaces.	

Defect ID: DEFECT000490783	
Technical Severity: Medium	Probability: Low
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: When the Management modules are upgraded to MR2, standby module unexpectedly reboots.	
Condition: The following conditions must apply: 1. More than 20 licenses are available in the system 2. Management module is upgraded to MR2 3. Applying a license while the system is not completely stable.	
Workaround: Delete the license that causes the issue and reapply it when the system is stable.	

Defect ID: DEFECT000491125	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: On deleting the BGP peer, SNMP snBgp4NeighborSummary table does not return data.	
Condition: SNMP 'snBgp4NeighborSummary' table does not return any data after deleting a peer.	
Recovery: A reload is necessary for the SNMP snBgp4NeighborSummary table to fetch data.	

Defect ID: DEFECT000491862	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Monitoring/RAS
Reported In Release: NI 05.6.00	Technology Area: Port Mirroring and Monitoring
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Traffic is not being mirrored to the proper ports, with a high CPU use as a result.	
Condition: When more than 2 ports are populated with 24x10G cards configured for in/out mirroring, the mirrored packets become corrupted.	

Defect ID: DEFECT000492934	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: NTP - Network Time Protocol
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: NTP server goes out of synchronization due to exceeded root distance.	
Condition: This issue is mostly seen in a scaled setup.	
Workaround: Remove the NTP servers and peers configuration then add it back. This clears the NTP statistical information of servers and peers.	

Defect ID: DEFECT000493253	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Traffic Management
Reported In Release: NI 05.3.00	Technology Area: Rate Limiting/Shaping
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: 1G ports forward fewer than the expected number of packets.	
Condition: When the port speed was changed to lower rates, shapers on those ports were set with those lower rates. These are not recovered when the ports go back to 1G.	

Defect ID: DEFECT000494399	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.4.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Unexpected reload on execution of 'debug packet-buffer' LP CLI command with a BR-MLX-10Gx24-DM module.	
Condition: When the LP CLI command 'debug packet-buffer' is executed on a BR-MLX-10Gx24-DM module, the line card will unexpectedly reload.	

Defect ID: DEFECT000494595	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.5.00	Technology Area: IEEE 802.1s MSTP
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Newly created VLANs do not participate in MSTP specifically when these VLANs are configured on CIST (i.e. instance 0) and MSTP enabled ports.	
Condition: Enable MSTP by adding VLANs to CIST (i.e. MSTP instance 0) even before creating these VLANs. Now create these VLANs and add member ports. These VLAN ports are not dynamically added to MSTP.	
Workaround: If the VLANs were added to any of the MSTP instances (except CIST) and then these VLANs were created, this issue is not seen.	
Recovery: Remove the VLANs in question from MSTP Instance 0 (i.e. CIST) and add it back. This would make the VLAN run MSTP on its member ports.	

Defect ID: DEFECT000495006	
Technical Severity: Low	Probability: High
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: HSBridge version required for 32 slot chassis in NI 5.6.00 is 17. Using HSBridge version 16 does not generate error or warning.	
Condition: On upgrade to NI 5.6.00, the HSBridge version as per configuration guide needs to be 17 and an error needs to be thrown on HSBridge version mismatch.	

Defect ID: DEFECT000496349	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Missing output for the 'show tech sfm' command after "Internal FE Tech-Support" section with a possible error message "No operational module in slot". This is seen if the node has more than one 100Gx2 or 10Gx24 module and the release is 5.6.00 or later.	
Condition: The node where the show tech output is requested will have more than one 100Gx2 or 10Gx24 module and 5.6.00 and later versions running.	

Defect ID: DEFECT000496594	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.7.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Traffic drops occur when traffic is running with port-port configurations at 100G line-rate with fixed 128B size.	
Condition: Must have line rate with fixed packet size of 128 Byte.	
Recovery: Reduce the traffic rate to match the expected throughput results.	

Defect ID: DEFECT000496669	
Technical Severity: High	
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.4.00	Technology Area: VRRP & VRRP-E (IPv6)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Symptoms may include either spotty communications or complete loss of communications within a few seconds after IPv6 VRRP failover.	
Condition: After reload and a subsequent IPv6 VRRP (VRRPv3) failover, the next backup becomes master and does not respond to IPv6 NS (neighbor solicitation) requests for the VRRPv3 VIP.	

Defect ID: DEFECT000497511	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: SDN
Reported In Release: NI 05.6.00	Technology Area: OpenFlow 1.0
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: After several days of adding and deleting flows continuously, traffic on a port starts getting dropped.	
Condition: This issue can happen on a node running software version 5.4.00 or above. It will only happen after a very large number of additions and deletions of flows (e.g., adding and deleting 500 flows every few minutes over 3 or 4 days).	

Defect ID: DEFECT000497688	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: The SNMP MIB object bgpPeerFsmEstablishedTime, which is used to get the Established time (Up time) of a BGP peer, will reset once every 50 days. This can result in different up time in the CLI vs SNMP.	
Condition: This issue is seen when the BGP peer is in the UP state for more than 50 days.	
Workaround: Use the SNMP MIB object bgp4V2PeerFsmEstablishedTime to see the correct up time of the BGP peer. This object is from an IETF draft BGPv4 MIB.	

Defect ID: DEFECT000498138	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: AAA
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: On change of username, the interface hangs and traffic does not flow in an MLX-4.	
Condition: SNMS task holds CPU for longer time than anticipated to validate the new password against the available history of passwords.	
Workaround: Clear the old passwords to reduce the validation time and avoid the interface hang and traffic loss.	
Recovery: - Use "no enable strict-password-enforcement". - Delete the user, and then re-add the same user to modify the password.	

Defect ID: DEFECT000498153	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: SDN
Reported In Release: NI 05.6.00	Technology Area: OpenFlow 1.0
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: While sending a packet-out to a switch where the packet-out had multiple output actions, only the first output action for a given packet-out is acted on within the switch.	
Condition: When multiple packet out actions are used, packets are not sent to multiple output ports.	

Defect ID: DEFECT000498623	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 2
Reported In Release: NI 05.4.00	Technology Area: Multi-Chassis Trunking
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: After reload/upgrade with the 'client-interfaces shut' config command, trying the 'no client-interfaces shut' command, the CCP does not come up.	
Condition: Upgrade with 'client-int shut' configured and try a 'no client-int shut' configuration, and the CCP does not come up.	
Recovery: Post the upgrade and after the 'no client-int shut', do a reload of MCT DUT, which had 'client-int shut' configured. This would not impact the traffic as the traffic would pass through the other MCT node.	

Defect ID: DEFECT000498762	
Technical Severity: Medium	
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.4.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: Pasting an encrypted SNMP community can fail to remove "public" as the default read-only community.	
Condition: The SNMP GET or WALK queries with the community "public" will be serviced, even though read-only communities are configured in the running configuration and "public" community is not.	
Workaround: The "no" keyword can be used to manually disable the default community (public). The CLI command is "no snmp-server community public ro".	
Recovery: Manually disable the default community (public).	

Defect ID: DEFECT000498960	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: TCP connection request to IPv4 broadcast or IPv6 anycast address results in a reply with a reset.	
Condition: When TCP connection is initiated to a IPv4 broadcast or IPv6 anycast address, the request is processed by TCP module in MP which then sends a reset message to the requesting node, thereby resulting in a security issue.	

Defect ID: DEFECT000498972	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.6.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: TCP connections for IPv6 subnet router anycast address are being processed and TCP reset is sent.	
Condition: When TCP connection is initiated to the device with IPv6 anycast address, the request is processed by MP CPU and a reset sent. This is the incorrect response. So by default no TCP reset will be sent.	

Defect ID: DEFECT000498977	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: SDN
Reported In Release: NI 05.6.00	Technology Area: OpenFlow 1.0
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: TCP connection to an openflow port on broadcast address needs to be blocked.	
Condition: When TCP connection to a openflow port is initiated with an IPv4 broadcast address, the request is processed by the MP CPU and a reset is sent. this is the incorrect response. Now, a TCP reset will not be sent in this scenario.	

Defect ID: DEFECT000498978	
Technical Severity: High	Probability: Medium
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.6.00	Technology Area: SNMPv2, SNMPv3 & MIBs
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: SNMP queries to IPv4 broadcast address are accepted. System should drop these requests.	
Condition: SNMP queries to IPv4 broadcast addresses get a valid response or authentication failures logs. System should not process these requests and instead drop the requests.	

Defect ID: DEFECT000498987	
Technical Severity: High	Probability: High
Product: Multi-Service IronWare	Technology: Layer 3
Reported In Release: NI 05.6.00	Technology Area: Static Routing (IPv6)
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: a) When the router is acting as the DHCP relay agent, the IPv6 static route installed at the relay agent as a result of DHCP REQUEST – ADVERTISE – REPLY sequence is removed after initial timeout period. b) When multiple DHCP servers respond with prefix addresses, every prefix address is installed in the IPv6 routing table when the router is acting as the DHCP relay agent. This can lead to mis-routing for the prefix(es) not accepted by the requesting DHCP client node.	
Condition: a) The DHCP client will continue to have the obtained address since the DHCP server responds to the clients renew request for the previously obtained address but the routing information at the DHCP relay agent will be lost during renewal sequence. b) Though the client receives responses from each DHCP server in the network, it will install only one address and silently ignore the remaining. But at the DHCP relay agent, it will keep every route which could potentially lead to mis-routing until any non-used routes time out eventually.	
Workaround: For the single DHCP server case, create a static route to the required prefixes. For the multiple DHCP servers case, avoid/remove the multiple DHCP server configuration at the DHCP client.	
Recovery: For single DHCP server cases, create a static route to the required prefixes. For multiple DHCP servers cases, avoid/remove the multiple DHCP server configuration at the DHCP client.	

Defect ID: DEFECT000500455	
Technical Severity: Low	
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.5.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: The last word in the error message "Error:port_calculate_count: unknown module tyoe" is misspelled. It should be "type".	
Condition: Configuring a non-existent module type over CLI session, the following error message is thrown in the console "Error:port_calculate_count: unknown module tyoe" with "type" mis-spelled.	

Defect ID: DEFECT000500457	
Technical Severity: Medium	Probability: Medium
Product: Multi-Service IronWare	Technology: Other
Reported In Release: NI 05.5.00	Technology Area: Other
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: The CLI command 'show module' will show a slot "Configured as <NULL> (127)" even though nothing shows up for the slot in the running config. "Error - module already configured at slot" is displayed when trying to add a module to the running config .	
Condition: Configuring an invalid module name will list the slot in "show module" and prevent other modules from being configured on the same slot.	
Workaround: Configure a valid module name.	
Recovery: Execute "no module" and configure a valid module name.	

Defect ID: DEFECT000502305	
Technical Severity: Medium	Probability: High
Product: Multi-Service IronWare	Technology: Management
Reported In Release: NI 05.6.00	Technology Area: SFLOW
Closed In Release(s): NI 05.6.00c(Fixed)	
Symptom: An incorrect raw packet header length in the sFlow protocol is observed.	
Condition: Issue is seen while running L3 traffic along while enabling sFlow on an interface. sFlow enabled interfaces send sFlow data packets to an sFlow collector. At the collector the raw packet header length is less than what was originally sent.	

Closed defects with code changes in R05.6.00b

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00b. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

This list has been updated for version 2 of the release notes. This list was closed on February 5, 2014.

Defect ID: DEFECT000473100	Technical Severity: Medium
Summary: When a static route pointing to null0 with distance 255 is configured, then the same static route with lower admin distance is not getting installed.	
Symptom: The route that is expected to be installed is not installed.	
Probability: Low	
Feature: IPv4 Static Route	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1221790

Defect ID: DEFECT000475917	Technical Severity: Medium
Summary: MLXe G2 modules can exhibit fabric link down due to loss of signal	
Symptom: Users may experience fabric link down in the following scenario ... found that RXSigDet (LOS) on both TM and FE side links were getting activated periodically indicating that loss of signal was being triggered and taking the links down.	
Probability: Medium	
Feature: System - XMR/MLX	Function: SFM
Reported In Release: NI 05.2.00	Service Request ID: 1197395

Defect ID: DEFECT000478534	Technical Severity: Medium
Summary: Show Optic output for 100G-CFP-ER4 is not correct.	
Symptom: Show Optic output for 100G-CFP-ER4 incorrectly shows 15 lanes, instead of 4.	
Probability: High	
Feature: MAC/PHY	Function: Optical Monitoring
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000479712	Technical Severity: Medium
Summary: Output of RMON stat command is not accounting packet size over 4049 byte in "oversize packets"	
Symptom: Seeing discrepancy in 'show rmon stat' output between the value of total packets and the sum of various packet sizes.	
Workaround: Use the command 'show stat' to display Giant packet counters instead..	
Feature: SNMP Management	Function: RMON Mib
Reported In Release: NI 05.4.00	Service Request ID: 1239207

Defect ID: DEFECT000480930	Technical Severity: Medium
Summary: Incorrect values on Y.1731 measurements when packets ingress and egress through different LPs	
Symptom: Y.1731 delay measurements and is seeing incorrect (negative) values being reported. The issue does not occur when packet ingress and egress interfaces are on the same LP.	
Probability: Medium	
Feature: 802.lag over VPLS	Function: Y.1731 PM - Delay Measurement
Reported In Release: NI 05.2.00	Service Request ID: 1246270

Defect ID: DEFECT000482831	Technical Severity: Medium
Summary: MP reset due to continuous port flaps	
Symptom: MP reset when a port was flapping continuously with OSPF configured on it.	
Probability: High	
Feature: System - XMR/MLX	Function: MP/LP I2C bus
Reported In Release: NI 05.2.00	Service Request ID: 1250386

Defect ID: DEFECT000483572	Technical Severity: High
Summary: ODL topology Discovery issue, extra 4 bytes found while Packet-in in MP for lldp packets sent from controller though packet out	
Symptom: ODL topology Discovery issue, where extra 4 bytes found while Packet-in in MP for lldp packets sent from controller though packet out	
Feature: Openflow 1.0	Function: Controller
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000484246	Technical Severity: Medium
Summary: Local fault is not flagged even though the remote fault is sent out.	
Symptom: In a 100G line card the LFS local fault is not flagged even though remote fault sent out.	
Feature: MAC/Phy	Function: link fault signalling
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000484964	Technical Severity: Critical
Summary: Bypass tunnel accounting does not work in case of ingress is same for bypass and protected FRR LSPs	
Symptom: Bypass tunnel accounting does not work in case of ingress is same for bypass and protected FRR LSPs	
Probability: High	
Feature: MPLS Control Plane	Function: Transit LSP Stats
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000485243	Technical Severity: Medium
Summary: After issuing the command 'no snmp-server community public ro' and issuing a 'wr mem' the configuration is still in the startup config after reload.	
Symptom: CLI command is not taking effect.	
Probability: Medium	
Feature: SNMP Management	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: 1255557

Defect ID: DEFECT000485609	Technical Severity: Critical
Summary: Mcache churning on router running 5.4.0dd during RP migration.	
Symptom: Number of mcache entries on the router keep oscillating without any changes in the network. Router running 5.4.0dd experienced mcache churning while migrating the RP to self from another router.	
Probability: Low	
Feature: IPv4-MC PIM-SM Routing	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1248593,1250814

Defect ID: DEFECT000486041	Technical Severity: High
Summary: Duplicate ACL entries are listed in L3 ACL Configuration Dialog while creating of a single IPv4 Standard/Extended ACL on 40G	
Symptom: Duplicate ACL entries are listed in L3 ACL Configuration Dialog while creating of a single IPv4 Standard/Extended ACL on 40G LP	
Workaround: Use CLI delete command with only sequence parameter	
Probability: High	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000486315	Technical Severity: Medium
Summary: IBGP neighbor using loopback from private VRF does not come up.	
Symptom: IBGP neighbor using loopback from private VRF stays in connected state.	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.5.00	Service Request ID: 1258144

Defect ID: DEFECT000486437	Technical Severity: High
Summary: After LSP flaps saw some MAC entries pointing to incorrect ports.	
Symptom: After LSP failover some of the MACs shows learned on incorrect port.	
Probability: Medium	
Feature: VPLS - XMR/MLX	Function: Forwarding - Single Tunnel
Reported In Release: NI 05.4.00	Service Request ID: 1259342

Defect ID: DEFECT000486808	Technical Severity: Medium
Summary: CER doesn't generate an PIM join when it receives an IGMP Membership report	
Symptom: PIM Join is not sent immediately after receiving IGMP group membership report	
Feature: PIM Neighbor filter	Function: PIM-SM
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000486957	Technical Severity: Medium
Summary: Pbif DOWNLOAD error in CES while copy through simplified upgrade in 5.6a	
Symptom: CES PBIF download issue when multi-threaded TFTP server is used.	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000487226	Technical Severity: High
Summary: MP reset at mpls_cu_process_soft_preempt_lsp_queue(pc), mpls_glue_task	
Symptom: MP reset with soft-preemption enabled.	
Workaround: Soft preemption disabled on LSPs	
Feature: RSVP-TE	Function: Soft-preemption
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000488056	Technical Severity: Medium
Summary: Error message "vlanu_add_port_mask() failed to add port mask to vlan 1" when removing Openflow configuration from interface, traffic stops forwarding.	
Symptom: After adding and removing Openflow configuration from an interface traffic stops forwarding.	
Workaround: Remove untagged port from vlan and re-add.	
Probability: High	
Feature: Openflow 1.0	Function: MLX L3 Forwarding
Reported In Release: NI 05.6.00	Service Request ID: 1267243

Defect ID: DEFECT000488303	Technical Severity: Medium
Summary: Out bound filtered FECs not showh correctly and peer not shown as upstream for the installed FECs for which out bound is applied	
Symptom: Out bound filtered FECs not shown correctly and peer not shown as upstream for the installed FECs for which out bound is applied	
Probability: Medium	
Feature: LDP	Function: FEC filtering
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000488336	Technical Severity: Critical
Summary: Openflow-1.3:LP reset @ of_hybrid_update_service_pram_for_ve(pc)	
Symptom: With port configured in hybrid port mode and a few flows added that are associated with that port then reloading the router caused the LP to reset.	
Probability: High	
Feature: Openflow 1.3	Function: MLX L3, L23, Hybrid
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000488408	Technical Severity: High
Summary: Clock-sync Mesh settings with FEC mode	
Symptom: It looks there are clock-sync issue with FEC mode if few(1/3) or less links are up in the device which causes new LP to go out-of-sync with other LP's in the system.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.6.00	Service Request ID: 736822

Defect ID: DEFECT000489335	Technical Severity: Critical
Summary: Reset observed on agent device while running a lexicographic SNMP testsuites using SNMPv2c get-next and get tests.	
Symptom: Reset observed on agent device while Performed the SNMPv2c testsuites for get-next and get operations after Configured interface based BFD session b/w two CER devices.	
Probability: High	
Feature: SNMP Management	Function: Routing Mib
Reported In Release: NI 05.6.00	

Defect ID: DEFECT000489790	Technical Severity: High
Summary: Rolling-reboot sets the LP that was found with mismatch version to Interactive, and causes LP Auto-upgrade to skip the upgrade for the LP	
Symptom: LP auto upgrade is broken for 8x10G and 2x100G modules when LP auto-upgrade command pointing to a 5.6 image with the system on a 5.6 application	
Probability: Medium	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Reported In Release: NI 05.6.00	Service Request ID: 1267344

Defect ID: DEFECT000490165	Technical Severity: Critical
Summary: System reset at mpls_clear_debug_summary(pc) while executing "cle mpls debug summary" from an SSH session	
Symptom: System reset at mpls_clear_debug_summary(pc) while executing "cle mpls debug summary" from an SSH session	
Probability: High	
Feature: MPLS Control Plane	Function: CLI
Reported In Release: NI 05.6.00	

NOTE: Customers with ACL and VPLS configuration on 2x100G cards should not upgrade to 5.600 or 5.600a. For details please refer to defect (DEFECT000487721).

Open Defects in R05.6.00a

This section lists open defects in Multi-Service IronWare R05.6.00a. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release that the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

NetIron 5.6.00 (9/30/2013) was released only to participants in the controlled Release program. NetIron 5.6.00a is the first generally available release.

The NetIron 5.6.00 release notes, as the initial feature release, contained Open, Closed with code, and Closed without Code defect lists. NetIron 5.6.00a is both a patch and first generally available NetIron 5.6.00 release, so it contains the Open, Closed with Code, and Closed without Code defect lists.

This list was generated on December 11, 2013

Defect ID: DEFECT000487721	Technical Severity: High
Summary: Traffic on a VPLS instance with ACLs stops passing traffic after reload on a 2x100G line card.	
Symptom: Traffic outage after reload. Issue limited to the following conditions: <ul style="list-style-type: none">- Applicable to 2x100G cards only. Does not affect any other cards.- Issue occurs only after reload of the line card or router.- Issue seen on VPLS endpoint and ACL config- Issue applicable to 5.6.00 and 5.6.00a releases only.	
Workaround: Re-bind the ACL on the interface.	
Feature: ACL - XMR/MLX	Function: L2 ACL
Reported In Release: NI 05.6.00	Probability: High

Defect ID: DEFECT000474227	Technical Severity: High
Summary: Scaled Multihop BFD sessions flap while learning 5k OSPF routes even with BFD timers set to 500ms	
Symptom: Scaled Multihop BFD sessions flap while learning 5k OSPF routes even with BFD timers set to 500ms	
Workaround: Workaround is to increase the BFD timers.	
Feature: BFD	Function: PROTOCOL
Reported In Release: NI 05.6.00	Probability: Low

Defect ID: DEFECT000476472	Technical Severity: High
Summary: OSPF is not removing more specific route in spite of the address is removed from the configuration.	
Symptom: OSPF is pointing to a wrong route (more specific route) in spite the address is being removed.	
Feature: OSPF	Function: PROTOCOL
Service Request ID: 1234642	
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000473898	Technical Severity: High
Summary: When a primary link of the RHP path on a member MLX flaps, then the primary link doesn't go to forwarding state upon receiving on RHP with forward bit set on its secondary interface	
Symptom: After a port flaps on a ring, the interface is not going to the forwarding state upon receiving RHP packet with forward bit set.	
Feature: L2 Protocol	Function: MRP2
Service Request ID: 1219422	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000474227	Technical Severity: High
Summary: Scaled Multihop BFD sessions flap while learning 5k OSPF routes even with BFD timers set to 500ms	
Symptom: Scaled Multihop BFD sessions flap while learning 5k OSPF routes even with BFD timers set to 500ms	
Workaround: Workaround is to increase the BFD timers.	
Feature: BFD	Function: PROTOCOL
Reported In Release: NI 05.6.00	Probability: Low

Defect ID: DEFECT000475917	Technical Severity: Medium
Summary: MLXe G2 modules can exhibit fabric link down due to LOS (loss of signal)	
Symptom: Customer experienced fabric link down in multiple systems. Found that RXSigDet (LOS) on both TM and FE side links were getting activated periodically indicating that loss of signal was being triggered and taking the links down. Each receiver always checks the amplitude of the signal against a minimum threshold. If the amplitude is detected to be less than the threshold the link is taken down, i.e. leaky bucket is set to 0. The threshold setting is called “LOSTH”, loss of signal threshold. By default it’s set to 0x16. Need a fix to lower the threshold to 0x10. This has been tested successfully in the customer's network. In the past, a value of 0x10, caused links not to come up intermittently at init. Vendor advises the solution is to only apply 0x10 value after links come up. Additional task is to prevent traffic from flowing until 0x10 value is applied. This should be applied on all TM fabric links (including those that to go FE13), all FE13 links, and all FE2 li	
Feature: System - XMR/MLX	Function: SFM
Service Request ID: 1197395	
Reported In Release: NI 05.2.00	

Defect ID: DEFECT000476498	Technical Severity: Medium
Summary: Latency seen in multicast traffic accompanied by TM logs	
Symptom: Customer has a multicast source connected to cisco switch which in-turn connects to MLX-16 port 2/1. There are multicast receivers connected all over this network. Running dense mode with 5.3e code results in the issue that video appearing as pixels. We are seeing lot of TM logs from various line cards as below: mailto:telnet@MLX-16#sh tm log Sep 12 02:43:23: Slot 7 PPCR 0 TM Reg offset 0x00001580 Value 0x00000002 Sep 12 02:41:27: Slot 1 PPCR 0 TM Reg offset 0x00001580 Value 0x00018002 Sep 12 02:41:26: Slot 2 PPCR 0 TM Reg offset 0x00001580 Value 0x00000003 Sep 12 02:41:10: Slot 3 PPCR 0 TM Reg offset 0x00001580 Value 0x00018002 SFM walk didn’t solve the issue.	
Feature: IPv4-MC PIM-DM Routing	Function: PERFORMANCE
Service Request ID: 1230366	
Reported In Release: NI 05.3.00	

Defect ID: DEFECT000478427	Technical Severity: Medium
Summary: BUM Traffic gets drop intermittently after CCEP port come Up when we flap the CCEP port.	
Symptom: In MCT VPLS environment When CCEP port is comes Up after disable /enable port, the BUM traffic gets dropped for 4 to 5 few secs and recovers fine after that.	
Feature: MCT	Function: Port Loop Detection
Service Request ID:	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000478534	Technical Severity: Medium
Summary: show optic output may not be correct for 100G-CFP-ER4	
Symptom: 15 lanes are displayed in "show optic" output for 100G-CFP-ER4, which has 3 lanes	
Feature: MAC/Phy	Function: Optical Monitoring
Service Request ID: 1239487	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000479712	Technical Severity: Medium
Summary: Output of rmon stat command is not accounting packet size over 4049 byte in "oversize packets"	
Symptom: Seeing discrepancy in show rmon stat output between the value of total packets and the sum of various packet size.	
Feature: SNMP Management	Function: RMON Mib
Service Request ID: 1239207	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000479829	Technical Severity: Medium
Summary: Duplicate mpls interface config seen for some interface	
Symptom: In the "router mpls" config section, the stanzas for mpls interface e1/[1 - 6] are duplicated, and the one for mpls interface e9/3 is not show, although that interface is in mpls protocol as per show commands: SSH@bx01.mrn02#show mpls interface e9/3 e9/3 (Trunk4) Admin: Up Oper: Up Maximum BW: 70000000 kbps, maximum reservable BW: 56000000 kbps (80%) Admin group: 0x40000001 (0 30) Reservable BW [priority] kbps: [0] 56000000 [1] 56000000 [2] 56000000 [3] 56000000 [4] 56000000 [5] 56000000 [6] 56000000 [7] 56000000 Last sent reservable BW [priority] kbps: [0] 56000000 [1] 56000000 [2] 56000000 [3] 56000000 [4] 56000000 [5] 56000000 [6] 56000000 [7] 56000000 LDP tunnel count: 0 Configured Protecting bypass lsps: 1 bypass_to_bx01.iad23(UP) <router mpls output showing duplicate interface entries for module 1 taken from customer show tech> <only partial output> router mpls mpls-interface e1/1 rsvp-reliable-messaging rsvp-refresh-reduction bundle-messa	
Feature: MPLS	Function: Application API
Service Request ID: 1243705	
Reported In Release: NI 05.2.00	

Defect ID: DEFECT000480930	Technical Severity: Medium
Summary: Incorrect values on Y.1731 measurements when packets ingress and egress through different LPs	
Symptom: Customer is doing Y.1731 delay measurements and is seeing incorrect (negative) values being reported.	
Feature: 802.lag over VPLS	Function: Y.1731 PM - Delay Measurement
Service Request ID: 1246270	
Reported In Release: NI 05.2.00	

Defect ID: DEFECT000483453	Technical Severity: Medium
Summary: The neighbor solicitation is continuously sent every second for 2 minutes, even after sending only 1 ping packet to a non-existing IPv6 address	
Symptom: Network is affected by constant multicast flooding, when MLXe sends 2 min of continuous ICMPv6-ND packets when trying to resolve non existing IPv6 hosts	
Workaround: Works in earlier versions, e.g. 5.2b (but seen in the latest 5.4 train)	
Feature: IPV6	Function: Neighbor Discovery
Service Request ID: 1246399	
Reported In Release: NI 05.4.00	Probability: High

Defect ID: DEFECT000484791	Technical Severity: Medium
Summary: non-zero privilege users are removed after a reload	
Symptom: User with non-zero privilege are deleted after a reload.	
Feature: AAA	Function: Local Authentication
Service Request ID: 1254493	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000475505	Technical Severity: Medium
Summary: MLX unexpectedly resets when adding tag interface list for all 24 ports on module to VPLS vlan.	
Symptom: Upgrade from NI 5200c to 5400d. After upgrade, upon reload, MLX unexpectedly resets when trying to load config. Wiped config via boot prompt, started pasting in configs. MLX has the same issue when trying to add the tagged interfaces in the VPLS vlan	
Feature: VPLS - XMR/MLX	Function: Control Plane
Service Request ID: 1231167	
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000454231	Technical Severity: Medium
Summary: After the configuration is copied via TFTP, the MPLS next-hop value may not be updated correctly.	
Symptom: Connectivity issues may occur after copying the configuration file using T ftp://ftp./	
Workaround: Do not copy the configuration via T ftp://ftp./ Recovery: Create static ARP entry for IP Next-Hop, which in turn creates the correct MPLS Next-hop.	
Feature: MPLS Forwarding - XMR/MLX	Function: Next-Hop Table
Service Request ID: 1165749	
Reported In Release: NI 05.2.00	Probability: Low

Defect ID: DEFECT000457684	Technical Severity: Medium
Summary: CES/CER is not updating the NHT table upon receiving gratuitous ARP from upstream firewall.	
Symptom: After failover, the device behind CES/CER cannot communicate.	
Feature: CES IPv4 Forwarding	Function: Next Hop Table
Service Request ID: 1168733	
Reported In Release: NI 05.4.00	Probability: Low

Defect ID: DEFECT000471322	Technical Severity: Medium
Summary: Not able to add more member VLANs to topology group	
Symptom: When adding multiple member VLAN to topology group, followed by “sh topology-group <group-id>” member-vlan shows NONE and “sh run” does not show any member-vlan.	
Feature: Topology Group	Function: VLAN Members
Service Request ID: 1194375	
Reported In Release: NI 05.0.00	Probability: Medium

Defect ID: DEFECT000471475	Technical Severity: Medium
Summary: CER/CES may hang or unexpectedly reload after the user password is changed.	
Symptom: This happens in rare conditions and appears to be dependent on the particular password value.	
Feature: Character I/O	Function: Character Handling
Service Request ID: 1212475	
Reported In Release: NI 05.4.00	Probability: Low

Defect ID: DEFECT000473100	Technical Severity: Medium
Summary: When a static route pointing to null0 with distance 255 is configured, then the same static route with lower admin distance is not getting installed.	
Symptom: The route that is expected to be installed is not installed.	
Feature: IPv4 Static Route	Function: PROTOCOL
Service Request ID: 1221790	
Reported In Release: NI 05.4.00	Probability: Low

Defect ID: DEFECT000473619	Technical Severity: Medium
Summary: max metric not going to active state on start-up wait for bgp when router id not configured explicitly	
Symptom: max metric not going to active state on start-up wait for bgp when router id not configured explicitly	
Workaround: configure routes id.	
Feature: OSPFv3	Function: PROTOCOL
Reported In Release: NI 05.6.00	Probability: Medium

Defect ID: DEFECT000474815	Technical Severity: Medium																																																	
Summary: BFD timer value for 150ms flap when system max mac value is configured for 2097152																																																		
Symptom: BFD timer value for 150ms flap when system max mac value is configured for 2097152. With this max mac config, Min time will always be around ~158 ms. If we are using Time-sensitive protocol less than 155ms, they will flap																																																		

With system-max mac as 2097152																																																		
LP-1#deb pro mac show																																																		
MAC Profiling Data Begin																																																		
<table><tr><td>Name</td><td>TotalTB</td><td>TotalMs</td><td>#ofCalls</td><td>MinUS</td><td>MaxUS</td><td>AvgUS</td></tr><tr><td>MAC_PROFILE_AGING</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td></tr><tr><td>MAC_PROFILE_FLUSH</td><td>79105735</td><td>3164</td><td>20</td><td>158005</td><td>158790</td><td>158211</td></tr><tr><td>MAC_PROFILE_LEARN</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td></tr><tr><td>MAC_PROFILE_ACTION_HANDLER</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MAC_PROFILE_INFO_MP</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td></td></tr><tr><td>MAC_PROFILE_FLUSH_MP</td><td>0</td><td></td><td></td><td></td><td></td><td></td></tr></table>		Name	TotalTB	TotalMs	#ofCalls	MinUS	MaxUS	AvgUS	MAC_PROFILE_AGING	0	0	0	0	0		MAC_PROFILE_FLUSH	79105735	3164	20	158005	158790	158211	MAC_PROFILE_LEARN	0	0	0	0	0		MAC_PROFILE_ACTION_HANDLER	0	0	0	0	0	0	MAC_PROFILE_INFO_MP	0	0	0	0	0		MAC_PROFILE_FLUSH_MP	0					
Name	TotalTB	TotalMs	#ofCalls	MinUS	MaxUS	AvgUS																																												
MAC_PROFILE_AGING	0	0	0	0	0																																													
MAC_PROFILE_FLUSH	79105735	3164	20	158005	158790	158211																																												
MAC_PROFILE_LEARN	0	0	0	0	0																																													
MAC_PROFILE_ACTION_HANDLER	0	0	0	0	0	0																																												
MAC_PROFILE_INFO_MP	0	0	0	0	0																																													
MAC_PROFILE_FLUSH_MP	0																																																	
Feature: System - XMR/MLX	Function: IPC/ITC																																																	
Reported In Release: NI 05.6.00	Probability: Low																																																	

Defect ID: DEFECT000475432	Technical Severity: Medium
Summary: SNMP trap uses an incorrect value (34 instead of 6 for 4 slot type) in snAgentBrdIndex.	
Symptom: The incorrect value will be displayed in TRAP message.	
Feature: SNMP Management	Function: System Management Mib
Service Request ID: 1211105	
Reported In Release: NI 05.4.00	Probability: Medium

Defect ID: DEFECT000476056	Technical Severity: Medium
Summary: Arrow card: MVID will be allocated when oif and core facing interfaces are physical	
Symptom: Arrow Card: MVID will be allocated when oif and core facing interfaces are physical	
Feature: IPv4-MC PIM-SM Routing	Function: PROTOCOL
Reported In Release: NI 05.6.00	Probability: Medium

Closed defects without code changes in R05.6.00a

This section lists defects closed without code changes in Multi-Service IronWare R05.6.00a.

Reported release indicates the product and release that the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

NetIron 5.6.00 (9/30/2013) was released only to participants in the controlled Release program. NetIron 5.6.00a is the first generally available release.

The NetIron 5.6.00 release notes, as the initial feature release, contained Open, Closed with code, and Closed without Code defect lists. NetIron 5.6.00a is both a patch and first generally available NetIron 5.6.00 release, so it contains the Open, Closed with Code, and Closed without Code defect lists.

This list was generated on December 5, 2013.

Defect ID: DEFECT000478245	Technical Severity: Critical
Summary: Some of the VE's stops learning MAC and ARP after reload.	
Symptom: When the system is reloaded. After a while we see that some of the VE's stop learning ARP/MAC.	
Reason Code: Not Reproducible	
Feature: IPv4 Forwarding - XMR/MLX	Function: ARP
Reported In Release: NI 05.5.00	Service Request ID: 1234625

Defect ID: DEFECT000416603	Technical Severity: High
Summary: L2 ACL based outbound rate limiting in VPLS instance may incorrectly rate limit other VLANs.	
Symptom: Packet loss in the VPLS VLANs where rate limiting is not applied, or is not hitting the rate limit.	
Reason Code: Not Applicable	Probability: Low
Feature: VPLS - XMR/MLX	Function: Data Plane
Reported In Release: NI 05.2.00	Service Request ID: 762203

Defect ID: DEFECT000423385	Technical Severity: High
Summary: ACL and QoS rate limit cannot be applied to the 4x10G module on fly.	
Symptom: Started to apply the ACL and rate limit QoS to the module NI-XMR-10Gx4. The applied rate limit did not take place: we had to power-off/on the 4x10G module.	
Workaround: Reboot the LP.	
Reason Code: Not Reproducible	Probability: Low
Feature: Rate Limiting - XMR/MLX	Function: IPv4 ACL-based
Reported In Release: NI 05.2.00	

Defect ID: DEFECT000426418	Technical Severity: High
Summary: Management module unexpectedly reloaded at task:hqos,function:m_avll_delete(pc) while copying the config from t ftp://ftp./	
Symptom: With dual management modules a switchover will occur. With only a single management module the entire system will reload.	
Reason Code: Will Not Fix	Probability: Low
Feature: HQoS	Function: Queue Management
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000430964	Technical Severity: High
Summary: Network LSAs are not exchanged properly with neighbors when VRFs are deleted & added using a script	
Symptom: Network LSAs are not exchanged properly with neighbors the VRFs are deleted & added using a script. In normal scenario, such an issue will not occur.	
Workaround: Clear ip ospf nei x.x.x.x.	
Reason Code: Not Reproducible	Probability: High
Feature: OSPF	Function: PROTOCOL
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000445124	Technical Severity: High
Summary: IPv6 ISIS is flapping when module configuration with open flow ports is removed from a different slot	
Reason Code: Already Fixed in Release	
Feature: Openflow Hybrid	Function: L2 mode
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000450373	Technical Severity: High
Summary: SFM links briefly down on 2x100 at module boot or init time.	
Symptom: No known symptoms, appears to be cosmetic in nature.	
Workaround: Upgrade to 5200g or higher, where the issue is not seen.	
Reason Code: Already Fixed in Release	Probability: Medium
Feature: System - XMR/MLX	Function: SFM
Reported In Release: NI 05.2.00	Service Request ID: 1145847

Defect ID: DEFECT000451385	Technical Severity: High
Summary: 10G link down due to a WAN PHY misalignment issue.	
Symptom: On rare occasions a 10G port physically configured for WAN mode and enabled may have a link down after system boot up.	
Reason Code: Will Not Fix	Probability: Low
Feature: CES Diagnostics	Function: Port Loopback Mode
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000461920	Technical Severity: High
Summary: Management switch-over followed by unexpected reboot.	
Reason Code: Not Applicable	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000464764	Technical Severity: High
Summary: External OSPF LSA database entry is present for a non-existent IP route.	
Symptom: The affected OSPF external LSA is getting propagated to other OSPF neighbors.	
Reason Code: Not Reproducible	
Feature: OSPF	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1192081

Defect ID: DEFECT000465703	Technical Severity: High
Summary: The device unexpectedly reloading in "bgp_RIB_out_delete_NLRI".	
Reason Code: Will Not Fix	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000468622	Technical Severity: High
Summary: Port is tied to non-existing VPLS id.	
Reason Code: Not Reproducible	
Feature: CES VPLS	Function: Forwarding
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000471220	Technical Severity: High
Summary: High CPU and 'Unexpected error: mcast set any AFI incorrect (35)' messages seen on console	
Reason Code: Not Applicable	
Feature: IPv4-MC PIM-DM Routing	Function: Forwarding - CES/CER
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000478870	Technical Severity: High
Summary: Unable to activate IPV6 neighbor under BGP 'address-family vpnv6 unicast'.	
Symptom: Seeing following error when trying to activate IPv6 neighbor under BGP 'address-family vpnv6 unicast'.	
'Address family not supported for IPv6 peer'	
Reason Code: Will Not Fix	
Feature: BGP	Function: BGPv6
Reported In Release: NI 05.5.00	Service Request ID: 1226863

Defect ID: DEFECT000486140	Technical Severity: High
Summary: After reload Power supply part number changed	
Symptom: After reload Power supply part number changed	
Reason Code: Not Applicable	
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: NI 05.2.00	Service Request ID: 1254861

Defect ID: DEFECT000406159	Technical Severity: Medium
Summary: ip ospf database-filter may not work when it is configured on more than two VEs.	
Symptom: ip ospf database-filter may not work when it is configured on more than two VEs.	
Reason Code: Not Reproducible	Probability: Low
Feature: OSPF	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 742311

Defect ID: DEFECT000427233	Technical Severity: Medium
Summary: PBIF issues with 5.4.0.0a code	
Reason Code: Not Reproducible	
Feature: FPGA	Function: PBIF
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000440728	Technical Severity: Medium
Summary: Unexpected fan error message displayed on teh 32-slot system	
Symptom: Cosmetic issue was seen at boot up "Error:rw_set_fan_led_gd: read_fan_controller_reg() PCA9554A_CMD_OUTPUT failed (ret = 64)" on a 32 slot chassis.	
Reason Code: Will Not Fix	Probability: Low
Feature: Infrastructure Utilities	Function: ITC
Reported In Release: NI 05.5.00	

Defect ID: DEFECT000441088	Technical Severity: Medium
Summary: Increase the maximum number of IPv6 Access Lists that can be configured on the MLX box.	
Reason Code: Not Applicable	
Feature: IPV6	Function: CONFIGURATION
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000448949	Technical Severity: Medium
Summary: TVF VLAN information and VLAN replacement is now supported for the 24x10 modules.	
Reason Code: Not Applicable	
Feature: PBR - XMR/MLX	Function: Preserve - VLAN
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000450312	Technical Severity: Medium
Summary: Not able to prepend Confederation As via Route map	
Reason Code: Not Applicable	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000451841	Technical Severity: Medium
Summary: Using the VLAN keyword in an ACL in conjunction with a TCP or UDP range keyword, does not retain the VLAN keyword.	
Reason Code: Already Fixed in Release	
Feature: Telemetry - XMR/MLX	Function: ACL with vlan-id
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000452841	Technical Severity: Medium
Summary: When a new port is added to a vlan, packets are not forwarded by the PBR policy configured on the ve interface.	
Symptom: Packets matching PBR configuration were not being forwarded to firewall.	
Workaround: Use 'ip rebind-acl all' command to clear condition.	
Reason Code: Not Reproducible	Probability: Medium
Feature: PBR - XMR/MLX	Function: IPv4
Reported In Release: NI 05.2.00	Service Request ID: 1158050

Defect ID: DEFECT000454183	Technical Severity: Medium
Summary: Auto upgrade feature fails to upgrade an FPGA image on a newly inserted module.	
Symptom: Received the following error when copying the FPGA image via TFTP: "Error:LP Upgrade: invalid XPP FPGA card type 1".	
Reason Code: Not Applicable	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Reported In Release: NI 05.3.00	Service Request ID: 1161752

Defect ID: DEFECT000455270	Technical Severity: Medium
Summary: In an L3VPN configuration the management module unexpectedly reloaded.	
Reason Code: Not Applicable	
Feature: Inter-VRF-Routing	Function: CONFIGURATION
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000457309	Technical Severity: Medium
Summary: MSDP peering did not re-establish after a system reboot.	
Symptom: MSDP was down after the reboot and had to be reconfigured before it would come up.	
Reason Code: Not Reproducible	Probability: High
Feature: IPv4-MC MSDP	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1106026

Defect ID: DEFECT000457332	Technical Severity: Medium
Summary: L4 rule-based CAM entry may not be released via SNMP SET(TFTP config download = snAgCfgLoad brcdIp.1.1.2.1.9).	
Reason Code: Already Fixed in Release	
Feature: SNMP Management	Function: Layer4 ACL-RL Mib
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000458515	Technical Severity: Medium
Summary: With vll-local configuration seeing unicast streams drops.	
Symptom: Seeing unicast VOD streams drop when there is a parallel lag connection for multicast streams.	
Reason Code: Not Reproducible	
Feature: CES VLL	Function: Local
Reported In Release: NI 05.0.00	Service Request ID: 1167255

Defect ID: DEFECT000459892	Technical Severity: Medium
Summary: Flow Statistic on controller is not working.	
Reason Code: Not Reproducible	
Feature: Openflow Extender	Function: Extender-Configuration
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000461559	Technical Severity: Medium
Summary: Only on systems running NI 5.2.00j, routes with no-export community are being announced to eBGP peers. NI 5.2.00j was the only released version containing this issue.	
Symptom: Routes with well-known communities are not being processed correctly, and may be incorrectly announced to other BGP peers, if an inbound route-map was used to modify the received BGP attributes. This occurs only on systems running NI 5.2.00j.	
Workaround: Use a route-map to filter out routes with a "no-export" community value. <p>The route-map filtering can filter any BGP community values, including the well-known community attributes.</p> <p>The following example shows how to filter out routes with the “no-export” community value:</p> <pre>ip community-list no-export-community-acl seq 5 permit no-export route-map customer-filter deny 1 match community no-export-community-acl route-map customer-filter permit 5</pre>	
Reason Code: Not Applicable	Probability: High
Feature: BGP	Function: BGPv4
Reported In Release: NI 05.2.00	Service Request ID: 1186974

Defect ID: DEFECT000462382	Technical Severity: Medium
Summary: acl-duplication-check restricts configuring permit/deny icmp any any 1/2/3	
Symptom: If "permit icmp any any 1" is configured, "permit icmp any any 2" statement cannot be configured.	
Reason Code: Already Fixed in Release	
Feature: ACL - XMR/MLX	Function: IPv6 ACL
Reported In Release: NI 05.5.00	Service Request ID: 1172392

Defect ID: DEFECT000463784	Technical Severity: Medium
Summary: Diag burn-in on a CES 2048CX running NI 5.4.00c fails intermittently.	
Reason Code: Not Reproducible	
Feature: Chassis/Hw Management	Function: Diagnostics (burn-in)
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000478064	Technical Severity: Medium
Summary: Syslog shows incorrect reason when port goes down.	
Reason Code: Not Applicable	
Feature: System - XMR/MLX	Function: Link Fault Signaling
Reported In Release: NI 05.4.00	

Closed defects with code changes in R05.6.00a

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00a. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

NetIron 5.6.00 (9/30/2013) was released only to participants in the controlled Release program. NetIron 5.6.00a is the first generally available release.

The NetIron 5.6.00 release notes, as the initial feature release, contained Open, Closed with code, and Closed without Code defect lists. NetIron 5.6.00a is both a patch and first generally available NetIron 5.6.00 release, so it contains the Open, Closed with Code, and Closed without Code defect lists.

This list was generated on December 12, 2013.

Defect ID: DEFECT000414410	Technical Severity: High
Summary: In a large OSPFv3 LSA environment, an LS update was retransmitted before the re-transmission interval expired.	
Symptom: The LS update was re-transmitted and the message "OSPFv3: Intf retransmit" appeared every 30 minutes.	
Feature: OSPFv3	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 753073

Defect ID: DEFECT000422796	Technical Severity: Critical
Summary: In rare cases after a reload the link between the TM and XPP may go down, resulting in LACP going into LACP-BLOCKED state.	
Symptom: Packet loss is observed affecting control and data packets.	
Feature: FPGA	Function: XPP-8x10
Reported In Release: NI 05.4.00	Service Request ID: ,1201023

Defect ID: DEFECT000425483	Technical Severity: High
Summary: A BGP neighbor outbound route update seems slow when updating/bringing up one peer in a large peer-group configuration.	
Symptom: The slowness is compared to the same operation on a smaller peer group configuration.	
Feature: BGP	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1090132

Defect ID: DEFECT000426116	Technical Severity: Medium
Summary: Experiencing multicast packet loss when forwarding from 1G to 10G interfaces.	
Symptom: Multicast traffic and CCM packets that transit CER/CES are intermittently dropped.	
Workaround: Put VPLS ports and MC port on the same Packet processor (port group).	
Feature: CES 802.1ag	Function: VPLS
Probability: Low	
Reported In Release: NI 05.1.00	Service Request ID: 1088924,1088924

Defect ID: DEFECT000431482	Technical Severity: Medium
Summary: Power-off 8x10 result in 2x100 OSPF link to get stuck in EXSTART/EXCHANGE state	
Symptom: Power-off 8x10 result in 2x100 OSPF link to get stuck in EXSTART/EXCHANGE state	
Feature: System - XMR/MLX	Function: SFM
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1085907

Defect ID: DEFECT000431900	Technical Severity: Medium
Summary: An ARP request from a particular source MAC failed to transmit between a pair of MLXs with a LAG configured between them.	
Symptom: In a very rare case, the ARP request for a particular MAC address did not get transmitted across the LAG.	
Workaround: Disable the affected LAG port that is the current Active Lead port, seen in 'sh lag'.	
Feature: L2 Forwarding - XMR/MLX	Function: MAC
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1109407

Defect ID: DEFECT000435843	Technical Severity: Critical
Summary: Under certain traffic pattern conditions with varying packet sizes, the data portion of the packet may be corrupted when traversing the 100G module.	
Symptom: After particular files are transferred, the checksum is incorrect. When this is observed, the traffic most often is characterized by jumbo packet sizes or non-jumbo packets at a very high traffic rate.	
Feature: IPv4 Forwarding - XMR/MLX	Function: MTU
Reported In Release: NI 05.4.00	Service Request ID: 1120693

Defect ID: DEFECT000436697	Technical Severity: High
Summary: In a specific situation, sending an edit-config RPC for MPLS using NetConf may lead to service interruption.	
Symptom: Reordering the RSVP and LSP containers in an RPC sent to a NetIron device may lead to a service interruption when debug output is redirected to a second SSH session and the LSP is being enabled in the RPC.	
Workaround: Reorder the mpls-config sub containers in the following order: path, lsp, rsvp.	
Feature: NetConf	Function: SSH Layer
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1126807,1126807

Defect ID: DEFECT000436705	Technical Severity: High
Summary: Using NetConf, the RSVP container exits before execution of the container leafs.	
Symptom: An edit-config RPC for mpls-config with an RSVP container does not execute.	
Workaround: Configure RSVP parameters using the normal CLI.	
Feature: NetConf	Function: Engine
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1126807

Defect ID: DEFECT000437901	Technical Severity: High
Summary: BGP convergence slow with outbound route-map applied to many members of a peer-group.	
Symptom: Route convergence slow outbound when peer-group contains many peers sharing the same route-map.	
Feature: BGP	Function: BGPv4
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1087001

Defect ID: DEFECT000438196	Technical Severity: Medium
Summary: QOS not marking CFM packets properly.	
Symptom: CFM packets may not be given the appropriate QOS value, based on the configuration.	
Feature: MPLS OAM	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1130330

Defect ID: DEFECT000438276	Technical Severity: Medium
Summary: In a rare situation a 4x10G module unexpectedly reloaded after adding a new VPLS instance to the configuration.	
Symptom: The service on the module will be interrupted for 1-2 minutes while the module reloads.	
Feature: MPLS	Function: Application API
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1131434

Defect ID: DEFECT000441972	Technical Severity: Medium
Summary: PIM Pruning Multicast stream although IGMP joins are still active but MLX timeout with KAT timer expired.	
Symptom: PIM Pruning Multicast stream although IGMP joins are still active but MLX timeout with KAT timer expired.	
Feature: IPv4-MC IGMP	Function: IGMPv3 Protocol
Reported In Release: NI 05.4.00	Service Request ID: 1121573

Defect ID: DEFECT000442150	Technical Severity: Medium
Summary: 100G port flaps randomly at least once every day.	
Symptom: Random port flaps: Jan 31 23:32:37:I:System: Interface ethernet 1/2, state up Jan 31 23:32:36:I:SYSTEM: port 1/2 is down(remote fault)	
Feature: System - XMR/MLX	Function: Link Fault Signaling
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1136028

Defect ID: DEFECT000442736	Technical Severity: Medium
Summary: The SNMP command 'snmpbulkwalk' is not using the outbound interface MTU.	
Symptom: snmpbulkwalk is using the global MTU setting, instead of the setting for the specific outbound interface MTU.	
Feature: IPv4	Function: UDP
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1138148

Defect ID: DEFECT000442993	Technical Severity: Medium
Summary: In specific configuration, after upgrading to 5300c, some ports are not transmitting any traffic.	
Symptom: Traffic between the Traffic manager and Packet processor is not getting forwarded causing connectivity issues	
Feature: FPGA	Function: XPP-48T/24Gx
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1139975

Defect ID: DEFECT000443139	Technical Severity: High
Summary: OSPF flap on 100G module insertion	
Symptom: After 2x100G module was inserted in slot 27, OSPF adjecencies on LP9 and LP21 unexpectedly flapped.	
Feature: OSPF	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1115968

Defect ID: DEFECT000443576	Technical Severity: Medium
Summary: Management module may unexpectedly reload while processing an RSVP-TE session.	
Symptom: If the system has dual management modules, the system will experience a switchover. If a single Management module is installed, then there will be service impact for about 3 minutes while the system reloads.	
Feature: MPLS Forwarding - XMR/MLX	Function: MPLS over VE
Probability: High	
Reported In Release: NI 05.3.00	Service Request ID: 1141311

Defect ID: DEFECT000443905	Technical Severity: Medium
Summary: Second Traffic Manager on 8x10G module is not able to forward traffic	
Symptom: For a particular 8x10G module, tower 2 TM ports are not able to learn ARP, so the traffic is not forwarded.	
Feature: TM/SFM	Function: Health monitoring
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1131599

Defect ID: DEFECT000444897	Technical Severity: Medium
Summary: In a rare case, an IPv6 forwarding problem occurs when the timing of a hardware addition was assessed incorrectly as a drop.	
Symptom: Connectivity issue seen with an IPv6 flow.	
Feature: IPv6 Forwarding - XMR/MLX	Function: Hardware Forward
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1144686

Defect ID: DEFECT000445099	Technical Severity: High
Summary: An interface module may have an unexpected reload processing an IPv6 ND when IPv6 neighbors reach the maximum allowable number.	
Symptom: The interface module will be impacted for 1 minute while the card reloads.	
Workaround: Upgrade to NI 05.4.00 code, where scaling for IPv6 ND is at 32k.	
Feature: IPV6	Function: Neighbor Discovery
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1145884

Defect ID: DEFECT000445526	Technical Severity: Medium
Summary: RSVP messages are sent on a less preferred route only (e.g., a default route), after deleting and adding the more specific route (e.g., /30).	
Symptom: PATH msg is forwarded to the less specific route's next-hop. If an RSVP destination is reachable via default route (0.0.0.0/0), it will not switch to use a better (more specific) route when a better route becomes available in RTM. This causes PATH msgs to get forwarded to the incorrect hop. The incorrect hop, upon receiving the PATH msg, will generate a PATH Error with "routing error", "top hop not it's local address" error. As a result, the LSP will not come up. Note that this issue is only applicable if RSVP is using a default route. Non default routes do not have this issue.	
Feature: RSVP-TE	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1145613

Defect ID: DEFECT000445590	Technical Severity: Medium
Summary: MCT KeepAlive control packet is not being forwarded if CER & MLX devices act as a pass-through.	
Symptom: The MCT KeepAlive control packet is dropped when the pass-through device is not configured with MCT.	
Feature: MCT	Function: CES_L2_FWD
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1130330

Defect ID: DEFECT000445872	Technical Severity: Medium
Summary: GRE Interface status from SNMP polling shows incorrect information for a disabled GRE tunnel interface.	
Symptom: Status is displayed as Up/Down, when the tunnel status is Down/Down.	
Feature: SNMP Management	Function: System Management Mib
Probability: High	
Reported In Release: NI 05.1.00	Service Request ID: 1137258

Defect ID: DEFECT000446451	Technical Severity: Medium
Summary: MLX not responding to LBM frames on local VPLS.	
Symptom: During OAM testing, the MLX is not responding to LBM frames on a local VPLS. It works properly if sent to a remote MEP.	
Workaround: If the down MEP is created on the connected port, it will work as expected. If it cannot be created on the connected port, the up MEP should be configured on the remote VPLS peer.	
Feature: PBB-OAM	Function: ESI
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: Case Number 1146909

Defect ID: DEFECT000446703	Technical Severity: Medium
Summary: 100G-CFP-10x10 optical modules may experience a random reset, causing a 1 second link flap.	
Symptom: The frequency between resets is typically days. When a CFP resets due to this issue, both sides of the link will report a link DOWN and a link UP event within a 1 second time stamp (i.e., link flap). It may or may not be accompanied by a Remote or Local Fault alarm, depending on the LFS setting and the type of transport equipment, if any, in-between. The link down/up status is available through the System Log and SNMP. Note that a link flap can be triggered by other reasons, such as an optical fiber cable issue, a transport equipment issue, or other faults.	
Workaround: This workaround should be performed during a maintenance window. The workaround will cause the link to go down and come back up. The workaround involves reading and writing registers to execute a sequence of initialization steps to put the CFP into the correct operational mode. In order for the workaround to be effective, the sequence must be run via a script so the timing between steps is well controlled. Remote access to the line card is required to execute the workaround. Brocade has a script available written for Tera Term version 4.7. Tera Term is a free open source terminal emulator available to the public. Please contact Brocade Support to coordinate a time to schedule a maintenance window and remote access to implement the workaround. After the terminal emulator is set up, the script takes approximately ten seconds per port to execute, and the actual down time on each port is approximately one second.	
Feature: MAC/Phy	Function: Link Status
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1148372,1149707

Defect ID: DEFECT000446756	Technical Severity: Medium
Summary: IPv4 and IPv6 route-maps with multiple "set next-hop" statements fail to acknowledge loss or recovery of the first next-hop when port ranges are used in the match condition ACL.	
Symptom: Packets are dropped instead of forwarded to a secondary next hop when a route-map's first configured next hop becomes unreachable.	
Workaround: For a temporary workaround, delete the "ip policy" or "ipv6 policy" config line from its interface then re-add it. This will last until the next time the reachability of the first next-hop changes. For a more permanent workaround, in IPv4 and IPv6 PBR route map match ACLs, never use port ranges and always use specific ports.	
Feature: PBR - XMR/MLX	Function: IPV6
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1148545

Defect ID: DEFECT000447028	Technical Severity: Medium
Summary: In a VPLS setup on a CER/CES platform, ether type 0x88E7 frames are dropped.	
Symptom: On a CER/CES platform, tagged L2 frames with ether type 0x88E7 may be dropped on an ingress port in a VPLS setup.	
Workaround: Configure the command below with an unused etype. tag-value isid <etype>	
Feature: CES VPLS	Function: Forwarding
Reported In Release: NI 05.4.00	Service Request ID: 1146588

Defect ID: DEFECT000447468	Technical Severity: Medium
Summary: Logging low RX power alarms/warnings when LOS is asserted (port is down).	
Symptom: 4x10G module with optical monitoring enabled for default of 3 minutes is logging alarms for a period of seconds. When the value is changed to 5 minutes, it is logging the alarm per the configured interval but it is restricted to only one port (logging alarm for port 1/1 alone). No logs for the other ports (1/2-1/4) though it has low alarm in "show optic 1" outputs.	
Feature: System - XMR/MLX	Function: Ethernet Optics
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1085737

Defect ID: DEFECT000448126	Technical Severity: Medium
Summary: By removing "CDP" and "FDP" from the config, "no cdp enable" and "no fdp enable" stayed in the config of VPLS end points, which cannot be removed.	
Symptom: CDP and FDP cannot be removed from the VPLS endpoints. If CDP and FDP are removed from the global config, the ports cannot be added in the LAG.	
Feature: FDP-CDP	Function: CLI
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1150164

Defect ID: DEFECT000448514	Technical Severity: Medium
Summary: In rare cases, the standby management module unexpectedly reloaded while processing licensing functionality with 2x100G module present.	
Symptom: In rare cases, the standby module was reloaded when the configuration was copied via SCP to a PCMCIA card and then copied to the running-config and a write mem executed. The unexpected reload happened when the Update License timer expired after the above config changes were applied.	
Workaround: The standby management module will reload and come back up without any impact to the existing traffic or functionality.	
Feature: SNMP Management	Function: Engine
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1151046

Defect ID: DEFECT000448774	Technical Severity: Medium
Summary: Inter VRF forwarding problem on a CES device.	
Symptom: Directly connected host on one VRF cannot reach another VRF.	
Feature: CES IPv4 Forwarding	Function: VRF-lite
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1143088

Defect ID: DEFECT000449925	Technical Severity: High
Summary: Client-interface shutdown does not keep all CCEP ports in disabled state after MCT node reload	
Symptom: After upgrading from 5.3 to 5.5, client-interfaces shutdown command was configured and then the device was reloaded. After the node came up, not all CCEP ports are in disabled state even though the running-config has the command in the cluster config.	
Workaround: Increase client-int delay to 120 sec or more.	
Feature: MCT-L2VPN	Function: Infrastructure
Probability: High	
Reported In Release: NI 05.5.00	Service Request ID: 1212893

Defect ID: DEFECT000449954	Technical Severity: Medium
Summary: TACACS+authorization commands which are not allowed to be run are able to be executed by a user if they are in an ACL editing context	
Symptom: Any commands made in ACL edit mode are not properly authenticated.	
Feature: AAA	Function: TACACS+ Authorization
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153064

Defect ID: DEFECT000449995	Technical Severity: Medium
Summary: MIB counter for "GoodOctets" is incorrect.	
Symptom: Command regarding MIB counter is giving a negative value for "GoodOctets" for both RX and TX.	
Feature: UNDETERMINED	Function: UNDER REVIEW
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1151090

Defect ID: DEFECT000450126	Technical Severity: High
Summary: LSP is torn down when a port for secondary FRR path goes down.	
Symptom: May receive log messages that the LSP Primary path went down.	
Feature: MPLS Control Plane	Function: LSP Manager
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1143968

Defect ID: DEFECT000450434	Technical Severity: High
Summary: 2x100G module throughput is not 100% on an MLX chassis.	
Symptom: When 100G traffic is sent through a 2x100G module, the OutUtilization is only ~63G in NORMAL mode and ~73% in TURBO mode.	
Feature: TM/SFM	Function: Performance (Throughput Latency)
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000451026	Technical Severity: Medium
Summary: In MCT over VPLS network some hosts can communicate while others cannot.	
Symptom: MCT over VPLS on the network and a few hosts cannot communicate across VPLS.	
Feature: MCT-VPLS	Function: CES-Hw Forwarding
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1155797,1152119

Defect ID: DEFECT000451642	Technical Severity: Medium
Summary: SSH users not timing out at configured "ip ssh idle-time".	
Symptom: SSH users are not timing-out after the configured ssh idle-timeout has expired. Example: ip ssh idle-time 15 SSH connections (inbound): 1 established, client ip address x.x.x.x, user is ssh1, privilege super-user using vrf default-vrf. 37 minutes 11 seconds in idle	
Feature: SSHv2	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1105020

Defect ID: DEFECT000451650	Technical Severity: Medium
Summary: Pings between Master and Backup VRRP are not working in a particular scenario.	
Symptom: Four boxes are connected in a rectangular configuration, spanning tree is disabled and one of the links is down. Unable to ping from VRRP Master ve to the Backup ve.	
Feature: VRRP	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1157380

Defect ID: DEFECT000451688	Technical Severity: Medium
Summary: After upgrading an MLXe-32 to NI 05.4.00b, SFM links go down and TM errors are seen.	
Symptom: SFM link disabled by system health monitor errors.	
Feature: TM/SFM	Function: Health monitoring
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1157797, 1132160

Defect ID: DEFECT000451855	Technical Severity: Medium
Summary: Multicast traffic loss may occur when an unrelated module is powered-off.	
Symptom: Multicast traffic loss is observed when an LP is powered off and that LP is not in the data path of the source and receiver.	
Feature: TM/SFM	Function: Forwarding - Multicast Traffic
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1157186

Defect ID: DEFECT000451898	Technical Severity: Medium
Summary: The "snAgSysLogGblCriticalLevel.0" OID (.1.3.6.1.4.1.1991.1.1.2.6.1.4.0) cannot be set to a value greater than 128.	
Symptom: The snChasWarningTemperature MIB does not read any values. The snAgSysLogGblCriticalLevel MIB cannot be set to a value greater than 128.	
Feature: SNMP Management	Function: System Management Mib
Reported In Release: NI 05.3.00	Service Request ID: 1157399

Defect ID: DEFECT000452455	Technical Severity: Medium
Summary: Port LED stays green when a CER/CES port configured "gig-default neg-off" is disabled using the CLI.	
Symptom: When a 1G interface with "gig-def neg-off" configured is disabled using the CLI, the port LED on the front panel stays green, even though the port is Down.	
Feature: CES SYSTEM	Function: PHY
Reported In Release: NI 05.4.00	Service Request ID: 1158705

Defect ID: DEFECT000452630	Technical Severity: Medium
Summary: When using the 'debug packet capture' command, the CER/CES does not strip the tag and sends a tagged packet on an untagged port configured as dual mode.	
Symptom: Unexpected result seen on the dual mode untagged port.	
Workaround: Run the command "no debug packet capture."	
Feature: L2 Forwarding - XMR/MLX	Function: Forwarding
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1158895

Defect ID: DEFECT000453085	Technical Severity: Medium
Summary: ACL is not working on port 7/1 and 7/4 but the same ACL is filtering traffic on 7/2 and 7/3.	
Symptom: ACL is not filtering traffic on port 7/1 and 7/4, which can cause security hole.	
Workaround: --	
Feature: ACL - XMR/MLX	Function: ACL policy
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1159069

Defect ID: DEFECT000453388	Technical Severity: Medium
Summary: CER/CES platform sends incorrect trap when the power supply unit is pulled from the chassis.	
Symptom: CER/CES sends snTrapChasPwrSupplyOK trap when the power supply unit is pulled from the chassis.	
Feature: SNMP Management	Function: Trap/Notification
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1155396

Defect ID: DEFECT000453549	Technical Severity: Medium
Summary: MLX may unexpectedly reload when shutting down a peer-group with more than 100 neighbors with 400K outbound routes for each neighbor.	
Symptom: The device was reloaded when the user shut down a peer group.	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1162827

Defect ID: DEFECT000453772	Technical Severity: Medium
Summary: Standby management module may reload while copying the config to the PCMCIA card.	
Symptom: There is no service impact when a standby management module reloads.	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1152758

Defect ID: DEFECT000453909	Technical Severity: High
Summary: Link keepalive configuration might not be parsed when upgrading from NI 5.2.00e to 5.3.00e if ports are part of a LAG.	
Symptom: When upgrading the device from NI 5.2.00e to 5.3.00e, some link-keepalive lines were not parsed causing the ports to stay down in the peers; and some devices were not working after the upgrade.	
Workaround: To recover, re-add the link-keepalive configuration for the missing ports.	
Feature: UDLD	Function: CLI
Probability: High	
Reported In Release: NI 05.3.00	Service Request ID: 1162695

Defect ID: DEFECT000453930	Technical Severity: Medium
Summary: When a port is removed from the LAG configuration, then the output of 'show vlan eth slot/port' shows the port is a member of configured VLANs on the system.	
Symptom: Shows incorrect information about the configured VLANs on the port.	
Feature: LAG - XMR/MLX	Function: Static
Reported In Release: NI 05.4.00	Service Request ID: 1165101

Defect ID: DEFECT000453941	Technical Severity: Medium
Summary: Provide information in show version' output that will indicate whether 1 port or 2 ports can be used (for 100G LP).	
Symptom: From the output of show version, it cannot be determined whether the module has 1 port or 2 port license.	
Feature: CLI Infrastructure	Function: Real Time Monitoring
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1135911

Defect ID: DEFECT000454040	Technical Severity: High
Summary: A 2x100 module will not support 100% line rate throughput on an MLX chassis.	
Symptom: A 2x100 module TM will see drops when sending line-rate traffic.	
Feature: System - XMR/MLX	Function: TM
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000454209	Technical Severity: Medium
Summary: Static IGMP group entries are aging out when the global multicast age is changed from the default.	
Symptom: When the multicast age was at 30 seconds, the static entry aged out.	
Feature: IPv4-MC IGMP	Function: IGMP static entries
Reported In Release: NI 05.4.00	Service Request ID: 1166157

Defect ID: DEFECT000454381	Technical Severity: Medium
Summary: Broadcast packet of VPLS link is not transmitted from LAG port after switchover.	
Symptom: Broadcast packet of VPLS link is not transmitted from LAG port after ESS MCT primary switchover.	
Workaround: Disable/enable the LAG port.	
Feature: MPLS Forwarding - XMR/MLX	Function: MPLS over LAG
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1154483

Defect ID: DEFECT000454509	Technical Severity: Critical
Summary: When Auto-Tuning is enabled, multicast packets may be dropped during the time that tuning is in progress.	
Symptom: Multicast packet loss might occur on some line cards during the auto-tuning process.	
Feature: TM/SFM	Function: Auto-tuning
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1161174

Defect ID: DEFECT000454591	Technical Severity: High
Summary: OSPF Session is resetting due to too many retransmissions	
Symptom: OSPF Session will flap and cause network impact.	
Feature: OSPF	Function: L3 VPN
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1165356

Defect ID: DEFECT000454936	Technical Severity: Medium
Summary: Cannot ping from host to host thru VLL.	
Symptom: When bringing up a cross-connect over a VLL, the interfaces and the VLL would come up, but the traffic did not make the connection.	
Workaround: Clear the ARP entry of the MPLS next hop. This refreshes the NHT entry.	
Feature: CES VLL	Function: Forwarding
Reported In Release: NI 05.2.00	Service Request ID: 1165243

Defect ID: DEFECT000454945	Technical Severity: Medium
Summary: VLL end-points are not passing LACP PDUs with forward-lacp configured if route-only is enabled globally.	
Symptom: LACP is not coming up across VLL.	
Feature: VLL - XMR/MLX	Function: VLL
Reported In Release: NI 05.2.00	Service Request ID: 1163591 and 1167145

Defect ID: DEFECT000455043	Technical Severity: Medium
Summary: DMM reflection on a local VPLS with multiple CE VLANs is not working.	
Symptom: When sending a DMR to a local VPLS MEP, there is no response if there are multiple VLAN IDs.	
Feature: MPLS OAM	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1166191

Defect ID: DEFECT000455228	Technical Severity: Medium
Summary: CLI and SNMP report a different number of temperature sensors for the 24x10G module.	
Symptom: The number of temperature sensors reported by the CLI command "show chassis" for the 24x10G module is not consistent with that of the SNMP report.	
Workaround: Use the "show chassis" CLI command to see the active sensors on the module.	
Feature: SNMP Management	Function: Engine
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1127000

Defect ID: DEFECT000455298	Technical Severity: Medium
Summary: MAC movement in VRF is not detected correctly.	
Symptom: After moving the host from one port to another in the same VLAN, the host is not reachable by a device from another VRF.	
Feature: CES IPv4 Forwarding	Function: VRF-lite
Reported In Release: NI 05.4.00	Service Request ID: 1166625

Defect ID: DEFECT000455315	Technical Severity: High
Summary: Elevated CPU utilization only on the Management module for the mcast and ip_receive task, with no service interruption.	
Symptom: Management sessions may be slowed down.	
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: NI 05.3.00	Service Request ID: 1166971

Defect ID: DEFECT000455478	Technical Severity: Medium
Summary: OSPF redistributed static routes disappear from OSPF neighbors.	
Symptom: OSPF routers stop receiving redistributed static routes from the neighbors.	
Feature: OSPF	Function: Redistribution
Reported In Release: NI 05.4.00	Service Request ID: 1161563 and 1169278

Defect ID: DEFECT000455612	Technical Severity: High
Summary: Unable to configure LDP-SYNC on Ethernet interface 1/1.	
Symptom: Unable to use the CLI to configure LDP Sync on Ethernet port 1/1.	
Workaround: Use port 1/1 as an untagged port in the VLAN and create a virtual interface.	
<pre> vlan 10 untagged ethe 1/1 router-interface ve 10 ! ! router ospf area 0 ldp-sync ! interface ve 10 ip ospf area 0 ip ospf network point-to-point ip ospf ldp-sync enable ip address xx.xx.xx.1/24 </pre>	
Feature: LDP	Function: LDP-IGP sync
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1154130

Defect ID: DEFECT000455817	Technical Severity: High
Summary: The tag values are not matching correctly with the route-map in the OSPF VRF distribute list.	
Symptom: The distribute list will not work as expected.	
Workaround: Do not use route-map with distribute-list for OSPF filtering. Use distribute-list with standard access-list alone. This creates an access-list and denies the specific prefixes, permitting the remaining ones. Example: Standard IP access list 21 deny 10.1.0.0 0.0.xxx.xxx deny 10.2.0.0 0.0.xxx.xxx permit any router ospf vrf test1 area 110 redistribute connected redistribute static route-map redid_map1 log adjacency distribute-list 21 in	
Feature: VRF	Function: CLI
Reported In Release: NI 05.1.00	Service Request ID: 1168149

Defect ID: DEFECT000455905	Technical Severity: High
Summary: Packet checksum errors causing IPv6 communication issues.	
Symptom: IPv6 NS for anycast address may trigger corruption in the NA reply packet.	
Workaround: Do not use IPv6 anycast address.	
Feature: IPV6	Function: Neighbor Discovery
Reported In Release: NI 05.4.00	Service Request ID: 1164891

Defect ID: DEFECT000456020	Technical Severity: Medium
Summary: Modified ACLs using TFTP may not work correctly when the ACL is being deleted at the global level and reconfigured using <u>Tftp://ftp./</u>	
Symptom: ACLs may not be applied properly, causing unexpected behavior.	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.4.00	Service Request ID: 1168434

Defect ID: DEFECT000456162	Technical Severity: High
Summary: IP packet is not transmitted from VE port in accordance with IP routing table.	
Symptom: Issue experienced while using Ping functionality.	
Feature: IPv4 Forwarding - XMR/MLX	Function: FIB
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1168193,1179903

Defect ID: DEFECT000456449	Technical Severity: High
Summary: Control packets should be given higher CPU priority so that lower priority packets cannot impact the control plane.	
Symptom: BFD and control plane impact noted: attempt to initiate an SSH session failed and OSPF flaps were observed.	
Feature: BFD	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1154675,1154675

Defect ID: DEFECT000456509	Technical Severity: Medium
Summary: After a software upgrade, an MLX32 MLX device is misrepresented as an XMR in the FDP output.	
Symptom: After a software upgrade, an MLX-3200 is shown as an XMR-32000.	
Feature: FDP-CDP	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1153498

Defect ID: DEFECT000456757	Technical Severity: Medium
Summary: When configuring the ipv6 ND reachable-time on an interface, "show ipv6 interface e <slot/port>" displays inconsistent output.	
Symptom: "show ipv6 interface e <slot/port>" displays ND reachable time incorrectly.	
Feature: IPV6	Function: Neighbor Discovery
Reported In Release: NI 05.4.00	Service Request ID: 1167966

Defect ID: DEFECT000456813	Technical Severity: Medium
Summary: LP 16 not forwarding traffic after MLXe-16 upgraded to 5.4.00bd	
Symptom: After upgrading router to 5.4.00bd ports on LP 16 were not forwarding traffic as expected.	
Workaround: Power cycle LP	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1169705

Defect ID: DEFECT000456977	Technical Severity: Medium
Summary: SNMP poll of OID 1.3.6.1.2.1.2.2.1.21 - ifOutQLen shows abnormally high values.	
Symptom: The high values do not correspond to the port statistics.	
Feature: SNMP Management	Function: Layer2 Mib
Reported In Release: NI 05.3.00	Service Request ID: 1166574

Defect ID: DEFECT000457469	Technical Severity: Medium
Summary: After reload the L4 CAM may not get programmed from a PBR configuration on the ingress module, causing unexpected forwarding results.	
Symptom: After upgrade, traffic is not being forwarded on all ports. The issue is specific to heavily loaded systems, with a PBR configuration. Systems with no PBR config are not susceptible to this issue. The issue can also happen on the reload of the whole system.	
Workaround: Follow the steps below to recover from the condition: 1. Remove pbr config. 2. Power cycle the module. 3. Reapply pbr config.	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1169233,1169233,1169

Defect ID: DEFECT000457665	Technical Severity: Medium
Summary: The response from remote MEPs is getting delayed because packets are trapped to the CPU at an intermediate node.	
Symptom: The delay in the MEP response may cause a link to go down, which may be service impacting.	
Feature: 802.1ag over VPLS	Function: CCM - Sub-second Timer
Reported In Release: NI 05.3.00	Service Request ID: 1150554

Defect ID: DEFECT000458550	Technical Severity: Medium
Summary: On the CER, an access-list configured with dscp-marking followed by drop-precedence is not working.	
Symptom: The expected behavior for the ACL is not seen.	
Feature: CES ACL	Function: L2 ACL
Reported In Release: NI 05.5.00	Service Request ID: 1169814

Defect ID: DEFECT000458561	Technical Severity: Medium
Summary: In case PIM is disabled, MP resets when pim dr-priority is configured to an interface	
Symptom: MP may reset unexpectedly when pim dr-priority value is configured from CLI.	
Feature: PIM Multinet	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: 1172077

Defect ID: DEFECT000458791	Technical Severity: High
Summary: Unable to telnet when “ip telnet source-interface loopback 1” is configured.	
Symptom: Error message: “Inactive source address” is received.	
Feature: Telnet Outbound	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1172497

Defect ID: DEFECT000458826	Technical Severity: Medium
Summary: Log message is not generated when OSPF LSA size exceeds the MTU size of the OSPF interface.	
Symptom: OSPFv3 LS Update with zero LSA , so the OSPF session flapped.	
Feature: OSPFv3	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1171792

Defect ID: DEFECT000458891	Technical Severity: Medium
Summary: The command ‘acl-duplication-check’ restricts configuring ‘deny ipv6 any any’ statement.	
Symptom: If ‘deny ipv6 any any routing-header-type 0’ is configured, ‘deny ipv6 any any’ statement cannot be configured.	
Feature: ACL - XMR/MLX	Function: IPv6 ACL
Reported In Release: NI 05.4.00	Service Request ID: 1172392

Defect ID: DEFECT000459019	Technical Severity: High
Summary: A rare specific bit pattern may cause CRC errors on the Serdes link of the 24x10 and 2x100 line cards.	
Symptom: This issue only happens in a rare circumstance caused by a specific data pattern on the BR-MLX-100Gx2-X and 24x10G linecards. If the Switch Fabric link goes down, there are redundant links available so there may be no impact.	
Feature: IPv4 Forwarding - XMR/MLX	Function: Hardware Forward
Reported In Release: NI 05.4.00	Service Request ID: 1172831

Defect ID: DEFECT000459272	Technical Severity: Medium
Summary: Issuing a LAG deploy after a PCMCIA copy command can cause the standby management modules to unexpectedly reload. If a switchover occurs after the PCMCIA copy, but before the LAG deploy, the active MP may reload.	
Symptom: An active management module unexpectedly reloads only after the following conditions are met: 1) Copying configuration from PCMCIA to running configuration. 2) Management module switchover. 3) LAG deploy. There is no service impact when a standby management module reloads. However, if the active management module reloads, a switchover will occur.	
Feature: Sflow - XMR/MLX	Function: General
Reported In Release: NI 05.2.00	Service Request ID: 1174886

Defect ID: DEFECT000459558	Technical Severity: Medium
Summary: MAC address of a neighbor device is learned on the monitor port when the "output or both" direction is configured.	
Symptom: When a port is configured as the monitor port for an "output or both" direction, the mac-address of a neighbor device connected to another port is learned on the monitor port:	
Feature: CES Mirroring	Function: Port Based
Reported In Release: NI 05.2.00	Service Request ID: 1172690

Defect ID: DEFECT000459817	Technical Severity: Medium
Summary: An interface unexpectedly reloaded due to TM Reset with Offset 0 and value of 0004.	
Symptom: The module will be impacted for 1-2 minutes while it reloads.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.3.00	Service Request ID: 1171573

Defect ID: DEFECT000460162	Technical Severity: High
Summary: 2x100G module throughput is not 100% on an MLX chassis.	
Symptom: When 100G traffic is sent through a 2x100G module, the OutUtilization is ~63G in Normal mode and ~73% in Turbo mode.	
Feature: TM/SFM	Function: Performance (Throughput Latency)
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000460394	Technical Severity: Medium
Summary: A CES/CER may unexpectedly reload after issuing a 'show ip' command if the following is configured: 'no ip source-route'; 'no ip icmp mpls-response' and 'no ip forward-protocol udp'.	
Symptom: The CES/CER will take a couple minutes to reload and traffic may be impacted if there is no alternate route.	
Feature: CES IPv4 Forwarding	Function: Routing
Reported In Release: NI 05.4.00	Service Request ID: 1184164

Defect ID: DEFECT000460551	Technical Severity: Medium
Summary: In Software version NI 5.5.00, the command "ipv6 nd global-suppress-ra" is not recognized as a valid command.	
Symptom: After upgrading to 5.5.00 the command "ipv6 nd global-suppress-ra" is no longer configured.	
Feature: IPV6	Function: Neighbor Discovery
Probability: High	
Reported In Release: NI 05.5.00	Service Request ID: 1183445

Defect ID: DEFECT000462097	Technical Severity: Medium
Summary: The device is unable to resolve a DNS name.	
Symptom: Sample output: telnet: abc.com Type Control-c to abort Sending DNS Query to a.b.c.d Ping Failed DNS: Errno(8) DNS query timed out...failed to resolve	
Feature: DNS	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1187621,1202936

Defect ID: DEFECT000462105	Technical Severity: Medium
Summary: After replacing a 4x10G module with an 8x10G, a LAG port in the 8x10G module does not function as expected.	
Symptom: The LAG port in the 8x10G module does not send out known unicast packets.	
Feature: LAG - XMR/MLX	Function: Static
Reported In Release: NI 05.2.00	Service Request ID: 1187833

Defect ID: DEFECT000462123	Technical Severity: High
Summary: In rare cases 2X100 LP boot, the TM initialization may fail and can cause unexpected LP reload	
Symptom: On 2X100 line card boot TM Health Monitoring detects an issue and can cause unexpected LP reload : "System: TM Health Monitoring detects an issue in slot 31 ppcr 0 Reg Offset 00000000 Value 00000004"	
Workaround: As the problem is only happen at boot time, it is safe to reset the card when TM access is blocked.	
Feature: Chassis/Hw Management	Function: Card/Chassis Management
Reported In Release: NI 05.5.00	Service Request ID: ,1255254,1187713

Defect ID: DEFECT000462367	Technical Severity: Medium
Summary: BGP Graceful Restart Speaker incorrectly generates TCP RST when it reloads itself.	
Symptom: When BGP Graceful Restart Speaker reloads, it generates a TCP RST to terminate the existing BGP session. The BGP Receiving Speaker then treats the routes learned via the session as Graceful routes; so these routes remain, even while the Graceful Restart Speaker is reloaded.	
Feature: BGP	Function: Graceful Restart
Reported In Release: NI 05.4.00	Service Request ID: 1187016

Defect ID: DEFECT000462494	Technical Severity: Medium
Summary: Device is not trying to resolve DNS name.	
Symptom: The sample output below indicates the device is not trying to resolve DNS; rather its response is as though it were working with an invalid IPV6 address. MLX#ping ipv6 abc Ping to IPV6 unspecified addresss not supported!	
Feature: IPV6	Function: ICMP
Reported In Release: NI 05.3.00	Service Request ID: 1188978

Defect ID: DEFECT000463069	Technical Severity: Medium
Summary: Priority force set on ingress port for CFM packets has an unexpected result.	
Symptom: CFM packet replies are missing the VLAN ID and the priority is changed.	
Feature: 802.lag over L2 VLANs	Function: INTEROPERABILITY
Reported In Release: NI 05.2.00	Service Request ID: 1149189

Defect ID: DEFECT000463219	Technical Severity: High
Summary: When 4 power supplies are powered-off on a 32-slot chassis, a fifth power supply fails.	
Symptom: When the fifth power supply fails, two line cards power off.	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1171527

Defect ID: DEFECT000463724	Technical Severity: High
Summary: In a rare condition, low priority traffic may be dropped in the presence of bursty high priority traffic at the ingress line cards (new generation 2x100, 4x40 and 24x10) due to aging.	
Symptom: Low priority traffic was getting dropped in spite of enough bandwidth on the egress port.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1187524

Defect ID: DEFECT000464152	Technical Severity: High
Summary: An unexpected 100GE Module TM Reset Recovery may be performed after an LP Power Cycle.	
Symptom: Additional TM reset causing longer interruption to traffic. Failure of TM to initialize correctly.	
Feature: TM/SFM	Function: TM Driver
Reported In Release: NI 05.4.00	Service Request ID: 1168132

Defect ID: DEFECT000464308	Technical Severity: Medium
Summary: Interface module memory depletes to less than 5% over a period of 6 to 8 months after an LP reboot.	
Symptom: A script is modifying the ACL two to three times every minute, but other devices running the same script do not experience the memory depletion.	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.2.00	Service Request ID: 1171022

Defect ID: DEFECT000464826	Technical Severity: High
Summary: Default route is not originated in to BGP	
Symptom: Default route is missing which can interrupt traffic.	
Workaround: This can be fixed by clearing the OSPF session at ao-e1-pe02 towards the Cisco router which triggers the default route to briefly disappear and then come back into the routing table.	
Feature: BGP	Function: Redistribution
Reported In Release: NI 05.4.00	Service Request ID: 1188142,1190574 / 11

Defect ID: DEFECT000464882	Technical Severity: Medium
Summary: Broadcast packets are looped when LAG ports are on different LPs.	
Symptom: A LAG port that is a VPLS endpoint advertises the MAC learned on another member port.	
Feature: VPLS - XMR/MLX	Function: Forwarding - Single Tunnel
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1193804

Defect ID: DEFECT000464893	Technical Severity: Medium
Summary: After a reload in certain configurations, the L4 ITC Message queue is filled by an aggressive refresh timer.	
Symptom: After reload or mass LP power-cycle, in certain configurations and hardware mixes, the IPv4 and IPv6 rule CAM may not get programmed for modules with PBR applied.	
Workaround: Power cycle each LP individually, waiting for each to come up individually.	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Reported In Release: NI 05.4.00	Service Request ID: 1169233

Defect ID: DEFECT000465088	Technical Severity: High
Summary: Support added for 64-bit timestamps for DMM measurements	
Symptom: Intermittent delays reported in DMM responses.	
Feature: 802.1ag over VPLS	Function: Y.1731 PM - Delay Measurement
Reported In Release: NI 05.3.00	Service Request ID: 1194219

Defect ID: DEFECT000465683	Technical Severity: High
Summary: Link-Keepalive may incorrectly disable the ports on slot 32 of an MLXe-32 chassis.	
Symptom: Ports are disabled by Link-Keepalive, interrupting traffic.	
Feature: UDLD	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1194842

Defect ID: DEFECT000466113	Technical Severity: High
Summary: After Reload with certain hardware and software configurations, FIDs may not be programmed correctly on some modules.	
Symptom: After Reload with certain HW and Software configurations, inconsistencies may result regarding FIDs.	
Workaround: Power cycle the affected interface modules one at a time.	
Feature: L2 Forwarding - XMR/MLX	Function: Forwarding
Reported In Release: NI 05.4.00	Service Request ID: 1169233

Defect ID: DEFECT000466291	Technical Severity: High
Summary: Multicast replication table may incorrectly utilize the resources and exhaust them in a scaled environment.	
Symptom: Some line cards may not receive multicast traffic.	
Feature: IPv4-MC PIM-SM Routing	Function: Forwarding - XMR/MLX
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1147574

Defect ID: DEFECT000466449	Technical Severity: High
Summary: BFD sessions flap while loading and removing BGP routes when BGP routing table is filled with 500K routes.	
Symptom: Large BGP updates causes high CPU resulting in BFD flaps.	
Feature: CES BFD	Function: OSPF
Reported In Release: NI 05.5.00	Service Request ID: 1246480

Defect ID: DEFECT000466486	Technical Severity: High
Summary: When forwarding jumbo packets or a sustained high utilization through a 100G module, corruption may occur due to some packet data that is missing.	
Symptom: Packet loss may occur and the TCP checksum will fail, requiring retransmission.	
Feature: FPGA	Function: XPP-8x10
Reported In Release: NI 05.4.00	Service Request ID: 1122271

Defect ID: DEFECT000466583	Technical Severity: High
Summary: An MBGP session over IPv6 neighbor resets due to an update containing MP_REACH_NLRI and no IPv4 update with a next_hop attribute at the end.	
Symptom: The BGP session will go down.	
Feature: BGP	Function: Multicast-BGP
Reported In Release: NI 05.2.00	Service Request ID: 1198324

Defect ID: DEFECT000467153	Technical Severity: Medium
Summary: Level-1 IPv6 prefixes are not automatically redistributed into Level-2.	
Symptom: L1 prefixes are not redistributed into L2, even though by default L1 prefixes should be automatically redistributed into L2.	
Feature: IS-IS	Function: Redistribution
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1185286

Defect ID: DEFECT000467383	Technical Severity: Medium
Summary: Console displaying error message every 5-10 minutes.	
Symptom: With SNMP polling enabled for 10-minute intervals, "ERROR:mplp_get_lp_data_request:Session65524: requested slot mask 00000001 00000000 is invalid" is displayed on the console every 5 - 10 minutes.	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1198189,1220700

Defect ID: DEFECT000467729	Technical Severity: Medium
Summary: No warning message is displayed when configured beyond the limitation of 512 VLL instances for CES.	
Symptom: CES currently allows creation of VLL instances beyond the limitation of 512 for both local and remote. No warning or error message is displayed.	
Feature: 802.1ag over VLL	Function: SCALABILITY
Reported In Release: NI 05.4.00	Service Request ID: 1186343

Defect ID: DEFECT000468056	Technical Severity: Medium
Summary: High MP CPU utilization from IGMP reports after upgrade	
Symptom: After upgrading from 4.x to 5.4, high CPU utilization from IGMP reports in VRF	
Feature: IPv4-MC PIM-SM Routing	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1187530,1211740

Defect ID: DEFECT000468739	Technical Severity: Critical
Summary: After hot insertion of a 24x10G module the last 8 ports (17-24) may not forward traffic correctly to some ports in the system.	
Symptom: Ports 17 to 24 may not forward traffic correctly to some ports, while they can forward to others just fine.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1187406

Defect ID: DEFECT000468956	Technical Severity: Medium
Summary: CER may experience an unexpected reload in SSH task.	
Symptom: The system will take 1-2 minutes to reload.	
Feature: SSHv2	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1206714

Defect ID: DEFECT000469125	Technical Severity: Medium
Summary: Additional debug code added for traffic forwarding issue.	
Symptom: Connectivity issue seen.	
Feature: IPv4 Forwarding - XMR/MLX	Function: ARP
Reported In Release: NI 05.4.00	Service Request ID: 1207062

Defect ID: DEFECT000469135	Technical Severity: Medium
Summary: LP auto-upgrade does not work for slot 32.	
Symptom: Inserted LP module into slot 32, after module came up FPGA code had not been updated to the correct version.	
Workaround: Insert module into another slot to upgrade images then move to slot 32 or boot into interactive mode and upgrade images manually.	
Feature: Infrastructure Utilities	Function: Image Copy / Download
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1205089

Defect ID: DEFECT000469240	Technical Severity: Medium
Summary: SNMP v3 does not accept AES encryption if AES password string starts with '00'.	
Symptom: When using AES password string that starts with '00' the command executes without an error but it does not show up in the configuration.	
Feature: SNMP Management	Function: Engine
Reported In Release: NI 05.3.00	Service Request ID: 1206017

Defect ID: DEFECT000469609	Technical Severity: Medium
Summary: In MCT+VPLS, Egress NP replicates broadcast / Multicast incorrectly.	
Symptom: In MCT+VPLS, Egress NP replicates broadcast / Multicast incorrectly after LP is powered off/on or reseated.	
Feature: MCT-VPLS	Function: Hardware Forwarding
Reported In Release: NI 05.4.00	Service Request ID: 1208602

Defect ID: DEFECT000469765	Technical Severity: High
Summary: Memory leak observed after upgrading to 5400c code.	
Symptom: Memory low on one of the CER switches -- "sh tech" does not show the running config .	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1209008

Defect ID: DEFECT000469866	Technical Severity: High
Summary: Inter VRF routing is not working for a loopback address.	
Symptom: Inter VRF routing is not working for a loopback address, so cannot reach to a loopback address in another VRF.	
Feature: IPv4 Forwarding - XMR/MLX	Function: VRF-lite
Reported In Release: NI 05.5.00	Service Request ID: 1208965

Defect ID: DEFECT000469899	Technical Severity: Medium
Summary: Power supply unit showing less watts compared to actual value in show chassis output	
Symptom: After upgrade from 5200fc to 5200fd the PSU3 AC value changed from 3000W to 2100W	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1209700

Defect ID: DEFECT000470361	Technical Severity: High
Summary: Removal of I2C retry debug messages	
Symptom: Multiple i2c set/clear messages reported in the logs.	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1209698

Defect ID: DEFECT000470570	Technical Severity: Critical
Summary: After modifying the primary LAG port very quickly on an MPLS interface, the changes are not getting reflected in the RSVP interface, which causes MPLS RESV message to drop.	
Symptom: Traffic loss across LSPs reported by monitoring system.	
Feature: MPLS Forwarding - XMR/MLX	Function: Transit LSR
Reported In Release: NI 05.2.00	Service Request ID: 1211401

Defect ID: DEFECT000471216	Technical Severity: High
Summary: Missing OSPF summary routes not being learned and after clearing OSPF neighbor, adjacency was stuck in Loading.	
Symptom: Some summarization routes are not learned.	
Feature: OSPF	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.5.00	Service Request ID: 1203985

Defect ID: DEFECT000471241	Technical Severity: Medium
Summary: Duplicate IP Address messages seen on master VRRP-E router.	
Symptom: Duplicate IP Addresses messages are seen in the logs of the master VRRP-E router when static route is configured pointing to the next hop interface that is on the same router as the virtual IP address.	
<p>Note:</p> <p>When VRRP-E node and a static route next hop share the same IP address, duplicate IP messages will be displayed three times in syslog in the following condition. This will be observed in XMR/MLX, CES/CER and CER-RT platforms.</p> <p>If VRRP-E is enabled in the presence of an installed static route and if the static route next hop happens to be the VRRP-E Virtual IP address, and if the VRRP-E node becomes the Master, duplicate IP messages will be displayed three times in syslog. This is due to the aging of the associated next-hop and ARP entry for the VRRP-E Virtual IP address. Till the point where the associated ARP entry is aged out, it continues to re-ARP and hence results in duplicate IP messages being displayed three times in syslog.</p>	
Feature: MCT	Function: VRRPE
Reported In Release: NI 05.4.00	Service Request ID: 1197426

Defect ID: DEFECT000471321	Technical Severity: High
Summary: Traffic is disrupted on even-numbered VLANs in a system with Gen1 cards and a large number of outbound ACLs configured.	
Symptom: Traffic disruption may manifest as <ul style="list-style-type: none"> - both nodes becoming master in VRRP/VRRP-e configuration, - MAC and ARP not being learned. The symptoms will be seen on even-numbered VLANs.	
Feature: L2 Forwarding - XMR/MLX	Function: Service-Type Table
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1209631

Defect ID: DEFECT000471366	Technical Severity: Medium
Summary: Diag burn-in on MP detects two kinds of failure	
Symptom: Diag burn-in on MP detects two kinds of failure. Issue 1) "hwPhyPortRegRead() read valid bit timeout 88E1145 PHY - Failed" Issue 2) "Port 13 passed Port 14 failed Port 15 passed Port 16 passed Port 17 passed Port 18 passed Port 19 passed Port 23 passed Dx246 Switch Port Loopback - Failed"	
Feature: System - XMR/MLX	Function: Diagnostics
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1210187

Defect ID: DEFECT000471645	Technical Severity: High
Summary: "client-interface delay" command only takes effect on primary LAG port	
Symptom: If the CCEP is an 802.1ad LAG, client-interface delay only takes effect on the primary port of the LAG. On non-primary port(s) the links comes up immediately.	
Feature: MCT	Function: LACP
Reported In Release: NI 05.4.00	Service Request ID: 1212893

Defect ID: DEFECT000471703	Technical Severity: Medium
Summary: Erroneous snAgentBrdIndex is set in snTrapModuleRemoved.	
Symptom: When removing Standby Management Module, erroneous snAgentBrdIndex is set over snTrapModuleRemoved. Erroneous snAgentBrdIndex is set only when 1st removing Standby Management Module after chassis comes up. The erroneous snAgentBrdIndex is seen only the 1st time removing Standby Management module: after that the correct snAgentBrdIndex.34 is set.	
Feature: SNMP Management	Function: Platform Mib
Reported In Release: NI 05.4.00	Service Request ID: 1211105

Defect ID: DEFECT000472111	Technical Severity: Critical
Summary: A packet is routed via VE over VPLS that has a route lookup hit of the destination network. When the hardware sends it to the CPU, it may trigger a reload of the ingress linecard.	
Symptom: There will be service impact to the ports on this interface module for about 1 minute while the module reloads.	
Workaround: Apply an inbound layer 3 access-list on the ve interface to deny the triggering traffic flow at the VPLS endpoint.	
Feature: Linecard / XPP	Function: PBIF TXA / RXA
Reported In Release: NI 05.4.00	Service Request ID: 1217702

Defect ID: DEFECT000472270	Technical Severity: High
Summary: NetIron does not re-converge link for external routes learned from NSSA areas.	
Symptom: After a link failure, the NSSA external routes are not getting converged to the correct outgoing interface and pointing to the down interface.	
Workaround: Remove NSSA area in this config & this issue will not be seen.	
Feature: OSPF	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1209617,1208650

Defect ID: DEFECT000472761	Technical Severity: Medium
Summary: DHCP offer packets are not sent out of the device	
Symptom: DHCP offer packets are being dropped on the MLX which is the default-gateway.	
Feature: IPv4 Forwarding - XMR/MLX	Function: Software Forward
Reported In Release: NI 05.4.00	Service Request ID: 1215264

Defect ID: DEFECT000472962	Technical Severity: High
Summary: BFD packets should be prioritized over UDP packets with TTL 1, so that BFD session might not flap.	
Symptom: An inbound flow of around 100mbps of UDP packets with a TTL of 1, the LP CPU usage was around 35% and BFD sessions flapped.	
Feature: CES SYSTEM	Function: Resource Manager
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1206930

Defect ID: DEFECT000472968	Technical Severity: Medium
Summary: Metro ring RHP packets are not forwarded until preforwarding timer expires	
Symptom: After CES link flaps the MRP ring master secondary port does not go into blocking until CES port goes into forwarding, causing network instability.	
Feature: L2 Protocol	Function: MRP1
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1219415,1219422

Defect ID: DEFECT000473019	Technical Severity: Medium
Summary: After removing VLANs from global config, OSPF redistribution stops working.	
Symptom: While deleting a VLAN, VE for the associated VLANs were first enabled and then disabled.	
Workaround: Do not run 'disable' the VE interface and instead, delete the applicable vlan.	
Feature: OSPF	Function: Redistribution
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1196686,1226632

Defect ID: DEFECT000474303	Technical Severity: Medium
Summary: The adjusted Maximum burst size for 1 Gbps - 10 Gbps should be 2,147,450,880 instead of the current 1,410,064,384	
Symptom: The problem is when average rate gets configured from 1Gbps to 10Gbps in CES platform.	
Feature: CES Rate Limiting	Function: Port Based
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1226361

Defect ID: DEFECT000474394	Technical Severity: Medium
Summary: XMR/MLX HTTPS web page XSS (Cross Site Scripting) security vulnerability	
Symptom: HTTPS web page susceptible to XSS security flaw, this is based on a known, public vulnerability.	
Feature: Web Management	Function: HTTP-SSL Engine
Reported In Release: NI 05.2.00	Service Request ID: 1218794

Defect ID: DEFECT000474492	Technical Severity: Medium
Summary: 1GE optics incorrectly recognized in 10GE cards.	
Symptom: They system will not properly notify user of incorrect optics being used in 10G module.	
Feature: MAC/Phy	Function: Optics Management
Reported In Release: NI 05.4.00	Service Request ID: 1225241

Defect ID: DEFECT000474577	Technical Severity: Medium
Summary: Incorrect diff value when attempting to do "show mem" after polling VPLS OID.	
Symptom: This situation does not happen when using SNMPv3 with noAuthNoPriv or when using SNMPv2c for the table walk . It is specific to the use of Auth with SNMPv3.	
Feature: SNMP Management	Function: System Management Mib
Reported In Release: NI 05.5.00	Service Request ID: 1226631

Defect ID: DEFECT000475266	Technical Severity: High
Summary: OSPF Infinite route cost with 16777215 is incorrectly installed in the database for summary LSA after a code upgrade.	
Symptom: This affected a particular network prefix for AREA 0 only. The same summary LSA is correctly passed to other areas with the correct metric.	
Workaround: Clearing the ospf route for the prefix resolves the issue.	
Feature: OSPF	Function: Flooding
Reported In Release: NI 05.4.00	Service Request ID: 1227115

Defect ID: DEFECT000475780	Technical Severity: Critical
Summary: When a CES/CER port is operating in half-duplex mode, this port may hang and ports in the same port group will be unable to transmit Multicast packets, affecting OSPF & VRRP for instance.	
Symptom: Protocols dependent on Multicast packets such as OSPF, VRRP-e and LACP may fail.	
Workaround: Avoid running in half-duplex mode.	
Feature: CES L2 Forwarding	Function: Protocol VLAN
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1228375,1228375

Defect ID: DEFECT000475804	Technical Severity: High
Summary: When pinging the management interface in the management vrf from a different subnet, the interface is unreachable.	
Symptom: The management interface is not reachable from a non-directly connected subnet.	
Feature: VRF	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: 1231311

Defect ID: DEFECT000475951	Technical Severity: Medium
Summary: Management module may unexpectedly reload when trying to generate RSA key.	
Symptom: If dual management modules are used a switchover will occur. Otherwise, with a single management module the system will perform a reload and service may be impacted for about 3 minutes.	
Feature: SSHv2	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1232622

Defect ID: DEFECT000476155	Technical Severity: High
Summary: When a unicast traffic flow returns to the MLX via a different LAG member, disabling/enabling that LAG port causes the return traffic to be dropped at the XPP.	
Symptom: Blackholing of the return traffic flow is observed.	
Feature: L2 Forwarding - XMR/MLX	Function: Forwarding
Reported In Release: NI 05.5.00	Service Request ID: 1212831

Defect ID: DEFECT000476247	Technical Severity: High
Summary: When multiple IP addresses are configured on a link, MLX is using incorrect IP address in TED database.	
Symptom: In multineted environment, when IP address at the remote router is removed, MLX is not updating a TED database correctly and using the old IP address in TED database.	
Feature: IS-IS	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1228374

Defect ID: DEFECT000476488	Technical Severity: Medium
Summary: LACP flap right after issuing 'show ip bgp routes sum' command.	
Symptom: Service impact may be experienced during LACP port flaps.	
Feature: BGP	Function: show commands
Reported In Release: NI 05.4.00	Service Request ID: 1215213

Defect ID: DEFECT000476898	Technical Severity: High
Summary: The standby management module does not accept the MCT "no client-interface shutdown" command and becomes out of sync with the active management module. It responds with the error "Wait for 30 sec to undo the client-interface shutdown"	
Symptom: Removing the client-interface shutdown command from the configuration on the active management module does not get synced with the standby management module and as a result client-interface shutdown is present in the configuration after a switchover.	
Feature: MCT	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: N/A

Defect ID: DEFECT000477636	Technical Severity: Medium
Summary: SSH with RSA keys do not get sync to Standby Management module after switchover.	
Symptom: After switchover SSH shows as disabled. MLXE-8#sh ip ssh SSH server status: Disabled	
Feature: SSHv2	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1238892

Defect ID: DEFECT000478132	Technical Severity: High
Summary: An interface module may reload unexpectedly as it is waiting for a print message that causes the watch dog time to hit and reload the card.	
Symptom: Ports on this module will be impacted for 1 minute while this module reloads.	
Feature: System - XMR/MLX	Function: Darter(Statistics and System SW)
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1239732

Defect ID: DEFECT000478430	Technical Severity: Critical
Summary: BUM is dropped for 100ms bidirectionally when ICL port (and CCP) goes down	
Symptom: BUM is dropped for 100ms bidirectionally when ICL port (and CCP) goes down	
Feature: TM/SFM	Function: Forwarding - Multicast Traffic
Reported In Release: NI 05.4.00	Service Request ID:

Defect ID: DEFECT000480429	Technical Severity: High
Summary: When link-error-disable is removed from ccep port on undeployed cluster, the link comes up.	
Symptom: Two issues here: <ul style="list-style-type: none"> 1) The customer had existing MCT cluster in a working condition. The customer had some issue with slot 1 and they wanted to replace the module. As a precaution they added port 2/2 in all the vlans including ICL (for which they got below error, which was expected). <p style="margin-left: 40px;">"Warning - port 2/2 is not ICL port currently and should not be added to cluster session vlan For proper cluster functionality convert the port to ICL port now"</p> <p>After replacing the module, the customer performed fail over (active management module to standby management module), which worked fine. Later, they decided to fail over again, the cluster became undeployed. The question is why the cluster became undeployed in the second reload.</p> 2) Link-error-disable is configured on CCEP port. If you undeploy the cluster and then remove command "link-error-disable" from the CCEP port, then the port gets enabled. This should not have happened. 	
Feature: MCT	Function: MLX_L2-FWD
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1239608

Defect ID: DEFECT000480546	Technical Severity: Medium
Summary: Ports fail to link up at one end, when using E1MG-LX-OM optics in a NI-MLX-1Gx20-SFP module.	
Symptom: When using E1MG-LX-OM optics in a NI-MLX-1Gx20-SFP module, ports fail to link up at one end after configuring gig-default neg-off and executing disable then enable.	
Feature: System - XMR/MLX	Function: Darter optics
Reported In Release: NI 05.4.00	Service Request ID: 1243669

Defect ID: DEFECT000481344	Technical Severity: High
Summary: The MPLS outbound tunnel is incorrectly programmed causing forwarding issues.	
Symptom: Traffic to certain prefix is not reachable due to outbound tunnel is incorrectly programmed.	
Feature: MPLS Forwarding - XMR/MLX	Function: L3VPN 2547
Reported In Release: NI 05.3.00	Service Request ID: 1248519

Defect ID: DEFECT000481597	Technical Severity: High
Summary: When ICL vlan is updated incorrectly and management module gets switch over, then cluster is getting deployed	
Symptom: Two issues here: 1) The customer had existing MCT cluster in a working condition. The customer had some issue with slot 1 and they wanted to replace the module. As a precaution they added port 2/2 in all the vlans including ICL (for which they got below error, which was expected). "Warning - port 2/2 is not ICL port currently and should not be added to cluster session vlan For proper cluster functionality convert the port to ICL port now" After replacing the module, the customer performed fail over (active management module to standby management module), which worked fine. Later, they decided to fail over again, the cluster became undeployed. The question is why the cluster became undeployed in the second reload. 2) Link-error-disable is configured on CCEP port. If you undeploy the cluster and then remove command "link-error-disable" from the CCEP port, then the port gets enabled. This should not have happened.	
Workaround: Un-deploy cluster	
Feature: MCT	Function: FSM
Reported In Release: NI 05.4.00	Service Request ID: 1239608

Defect ID: DEFECT000481998	Technical Severity: Medium
Summary: Error Not thrown to Telnet session when IP receive access-list is not applied correctly due to lack of CAM space	
Symptom: Error Not thrown to Telnet session when IP receive access-list is not applied correctly due to lack of CAM space	
Workaround: Increase system-max receive-cam size	
Feature: ACL - XMR/MLX	Function: rACL
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1244112

Defect ID: DEFECT000482102	Technical Severity: Medium
Summary: ISIS not learning loopback /32 route from peer after metric changes were made.	
Symptom: Unable to learn ISIS routes in one of routers for the loopback IP of other router after changing metric costs. After changes were reverted the problem remained.	
Feature: IS-IS	Function: Redistribution
Reported In Release: NI 05.4.00	Service Request ID: 1249617,1249617

Defect ID: DEFECT000482336	Technical Severity: High
Summary: We observed that the Oif timer memory pool had been exhausted on the distribution switch. Potentially, this can lead to a lot of stale OIFs that never age out.	
Symptom: The oif in the mcache entry was not getting removed.	
Vrf Instance : default-vrf	

	allocated in-use available allo-fail up-limit
NBR list	256 46 210 0 512
RP set list	256 0 256 0 1536
Static RP	64 1 63 0 64
LIF Entry	512 0 512 0 512
Anycast RP	64 0 64 0 64
timer	256 19 237 0 no-limit
prune	128 0 128 0 no-limit
pimsm J/P elem	27590 1 27589 0 65535
pimsm J/P group	2513 1 2512 0 65535
Timer Data	221184 221184 0 245624897 no-limit
mcache	10335 10097 238 0 no-limit
graft if no	
Feature: IPv4-MC PIM-SM Routing	Function: Forwarding - XMR/MLX
Reported In Release: NI 05.4.00	Service Request ID: 1241979

Defect ID: DEFECT000482798	Technical Severity: High
Summary: Some of the ports are in Designated Discarding	
Symptom: Some of the ports which is suppose to be forwarding are showing as ' DESIGNATED DISCARDING '	
3/3 128 2000 T F DESIGNATED DISCARDING 2000 1000748ef8248967	
Feature: L2 Protocol	Function: RSTP
Reported In Release: NI 05.4.00	Service Request ID: 1251006

Defect ID: DEFECT000483904	Technical Severity: Medium
Summary: "drop-precedence force" doesn't work unless reloading the box	
Symptom: In order to apply "drop-precedence force" on the box, we have to reload the box. Although turning off "drop-precedence force" doesn't need the reload.	
Workaround: Reload the box.	
Feature: CES QOS	Function: Port Prioritization
Reported In Release: NI 05.2.00	Service Request ID: 1253387

Defect ID: DEFECT000485243	Technical Severity: Medium
Summary: 5400e : Customer can remove "snmp read-only" community . Community ro appears in the config after reload.	
Symptom: 5400e : Customer can remove "snmp read-only" community . Community ro appears in the config after reload. Also if it appears in the box after reboot then why it is allowing teh customer to remove the community .	
Feature: SNMP Management	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: 1255557

Defect ID: DEFECT000485488	Technical Severity: Critical
Summary: UDLD goes down after exceeding LP system uptime of 621 days.	
Symptom: UDLD goes down after exceeding LP system uptime of 621 days.	
Workaround: MP reboot,LP reboot, interval>3	
Feature: UDLD	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1256917

Open Defects in R05.6.00

This section lists open defects in Multi-Service IronWare R05.6.00. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release that the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

This list was generated on September 24, 2013

Defect ID:	DEFECT000475780	Technical Severity: Critical
Summary:	With NI 5.2.00f, CER stops forwarding multicast traffic, causing OSPF and VRRP-e to fail.	
Symptom:	<p>Ve 403 (vlan 404 untagged eth 1/44) RTR 14 connects to port 1/33 of Vlan 403 (untagged eth 1/33) of RTR15 .Ospf is not coming up fine. And is stuck in init state. This time RTR14 is not processing any multicast packets.</p> <p>V68 (1/27) on RTR14 and RTR15 are connected to L2 switch and l2 switch is connected to end customer . VRRP-e is master on both the sides for ve 68.</p> <p>V103(1/31) on RTR14 and RTR15 are connected to another L2 switch and l2 switch is connected to end customer . VRRP-e is a master for both the sides for ve 103.</p> <p>V214 (1/30) on RTR14 and RTR15 are connected to another L2 switch and l2 switch is connected to end customer . VRRP-e is a master for both the sides for ve 214.</p> <p>V99 (1/26) on RTR14 and RTR15 are connected to another L2 switch and l2 switch is connected to end customer . VRRP-e is a master for both the sides for ve 99.</p> <p>V410 (1/42) on RTR14 and RTR15 are connected to another L2 switch and l2 switch is connected to end customer.</p>	
Workaround:	Avoid running copper port in half duplex mode.	
Feature:	CES L2 Forwarding	Function: Protocol VLAN
Service Request ID:	1228375,1228375	
Reported In Release:	NI 05.2.00	Probability: High

Defect ID:	DEFECT000476247	Technical Severity: High
Summary:	When multiple IP addresses are configured on a link, MLX is using incorrect IP address in TED database.	
Symptom:	In multineted environment, when IP address at the remote router is removed, MLX is not updating a TED database correctly and using the old IP address in TED database.	
Feature:	IS-IS	Function: PROTOCOL
Service Request ID:	1228374	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000465088	Technical Severity: High
Summary:	Support added for 64-bit timestamps for DMM measurements	
Symptom:	Intermittent delays reported in DMM responses.	
Feature:	802.1ag over VPLS	Function: Y.1731 PM - Delay Measurement
Service Request ID:	1194219	
Reported In Release:	NI 05.3.00	

Defect ID:	DEFECT000462063	Technical Severity: High
Summary:	Follow on traffic loss on FRR LSPs after link failure - duration is up to 16 minutes	
Feature:	MPLS Control Plane	Function: Adaptive FRR
Reported In Release:	NI 05.6.00	Probability: Medium

Defect ID:	DEFECT000466291	Technical Severity: High
Summary:	Multicast replication table may incorrectly utilize the resources and exhaust them in a scaled environment.	
Symptom:	Some line cards may not receive multicast traffic.	
Feature:	IPv4-MC PIM-SM Routing	Function: Forwarding - XMR/MLX
Service Request ID:	1147574	
Reported In Release:	NI 05.3.00	Probability: Low

Defect ID:	DEFECT000471216	Technical Severity: High
Summary:	Missing OSPF routes and low MP buffer	
Symptom:	Received routes are not installed in the route table.	
Feature:	OSPF	Function: PROTOCOL
Service Request ID:	1203985	
Reported In Release:	NI 05.5.00	Probability: Medium

Defect ID:	DEFECT000471860	Technical Severity: High
Summary:	PIMDM Basic test - Seeing traffic TX at double rate than expected on lag ports.	
Feature:	IPv4-MC PIM-DM Routing	Function: Forwarding - XMR/MLX
Reported In Release:	NI 05.6.00	Probability: Medium

Defect ID:	DEFECT000472270	Technical Severity: High
Summary:	NetIron does not re-converge link for external routes learned from NSSA areas.	
Symptom:	After a link failure, the NSSA external routes are not getting converged to the correct outgoing interface and pointing to the down interface.	
Workaround:	Remove NSSA area in this config & this issue will not be seen.	
Feature:	OSPF	Function: PROTOCOL
Service Request ID:	1209617,1208650	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000472962	Technical Severity: High
Summary:	BFD packets are not scheduled ahead of UDP packets with TTL 1 and therefore BFD sessions are flapping	
Symptom:	An inbound flow of around 100mbit of UDP packets with a TTL of 1. LP CPU usage was around 35% and all BFD sessions terminating on the same module were flapping approx every 10 seconds.	
Workaround:	dm metro 0 cpu_code 144 256	
Feature:	CES SYSTEM	Function: Resource Manager
Service Request ID:	1206930	
Reported In Release:	NI 05.2.00	Probability: Medium

Defect ID:	DEFECT000475544	Technical Severity: High
Summary:	Not able to install more than 4K flows via SSL session without connection being reset. 1 SSL session, 4K + flows	
Symptom:	Session resets while flows are being installed via SSL session. This way customer would not be able to install more than 4K flows in one shot and would have to send flows separately 4K at a time.	
Workaround:	The flows should be divided into chunks of 4k or less. The controller should send one chunk of flows and send echo request. On getting echo response, it should send the next chunk.	
Feature:	Openflow 1.0	Function: SSL
Reported In Release:	NI 05.6.00	Probability: Medium

Defect ID:	DEFECT000475897	Technical Severity: High
Summary:	Multiple DUTs report power supply issues after boot up on 5600b360	
Feature:	Chassis/Hw Management	Function: i2c - Power supply
Reported In Release:	NI 05.6.00	Probability: Low

Defect ID:	DEFECT000467153	Technical Severity: Medium
Summary:	Level-1 IPv6 prefixes are not automatically redistributed into Level-2.	
Symptom:	L1 prefixes are not redistributed into L2, even though by default L1 prefixes should be automatically redistributed into L2.	
Feature:	IS-IS	Function: Redistribution
Service Request ID:	1185286	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000474394	Technical Severity: Medium
Summary:	XMR/MLX HTTPS web page XSS (Cross Site Scripting) security vulnerability	
Symptom:	HTTPS web page susceptible to XSS security flaw, this is based on a known, public vulnerability.	
Feature:	Web Management	Function: HTTP-SSL Engine
Service Request ID:	1218794	
Reported In Release:	NI 05.2.00	

Defect ID:	DEFECT000447028	Technical Severity: Medium
Summary:	In a VPLS setup on a CER/CES platform, ether type 0x88E7 frames are dropped.	
Symptom:	On a CER/CES platform, tagged L2 frames with ether type 0x88E7 may be dropped on an ingress port in a VPLS setup.	
Workaround:	Configure the command below with an unused etype. tag-value isid <etype>	
Feature:	CES VPLS	Function: Forwarding
Service Request ID:	1146588	
Reported In Release:	NI 05.4.00	

Defect ID:	DEFECT000475432	Technical Severity: Medium
Summary:	SNMP trap uses a incorrect value (34 instead of 6 for 4 slot type) in snAgentBrdIndex	
Symptom:	snAgentBrdIndex uses 34 even in 4 slot type, not 6. In 32 slot type, Standby MGMT uses 34 for snAgentBrdIndex(OID 1.3.6.1.4.1.1991.1.1.2.2.1.1.1). Because 1-32 is LP, 33-34 is for MP and 35-42 is for SFM are reserved. 4 slot type: 1-4 is for LP, 5 and 6 is MP, 7-9 is SFM and I expected standby MGMT in 4 slot type uses 6. However actually 34 is still used even in 4 slot type.	
Feature:	SNMP Management	Function: System Management Mib
Service Request ID:	1211105	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000475505	Technical Severity: Medium
Summary:	MLX unexpectedly resets when adding tag interface list for all 24 ports on module to VPLS vlan.	
Symptom:	Upgrade from NI 5200c to 5400d. After upgrade, upon reload, MLX unexpectedly resets when trying to load config. Wiped config via boot prompt, started pasting in configs. MLX has the same issue when trying to add the tagged interfaces in the VPLS vlan.	
Feature:	VPLS - XMR/MLX	Function: Control Plane
Service Request ID:	1231167	
Reported In Release:	NI 05.4.00	

Defect ID:	DEFECT000451650	Technical Severity: Medium
Summary:	Pings between Master and Backup VRRP are not working in a particular scenario.	
Symptom:	Four boxes are connected in a rectangular configuration, spanning tree is disabled and one of the links is down. Unable to ping from VRRP Master ve to the Backup ve.	
Feature:	VRRP	Function: PROTOCOL
Service Request ID:	1157380	
Reported In Release:	NI 05.4.00	Probability: Low

Defect ID:	DEFECT000454231	Technical Severity: Medium
Summary:	After the configuration is copied via TFTP, the MPLS next-hop value may not be updated correctly.	
Symptom:	Connectivity issues may occur after copying the configuration file using TFTP.	
Workaround:	Do not copy the configuration via TFTP. Recovery: Create static ARP entry for IP Next-Hop, which in turn creates the correct MPLS Next-hop.	
Feature:	MPLS Forwarding - XMR/MLX	Function: Next-Hop Table
Service Request ID:	1165749	
Reported In Release:	NI 05.2.00	Probability: Low

Defect ID:	DEFECT000457684	Technical Severity: Medium
Summary:	CES/CER is not updating the NHT table upon receiving gratuitous ARP from upstream firewall.	
Symptom:	After failover, the device behind CES/CER cannot communicate.	
Feature:	CES IPv4 Forwarding	Function: Next Hop Table
Service Request ID:	1168733	
Reported In Release:	NI 05.4.00	Probability: Low

Defect ID:	DEFECT000471322	Technical Severity: Medium
Summary:	Not able to add more member vlans to topology group	
Symptom:	When adding multiple member vlan to topology group, followed by "sh topology-group <group-id>" member-vlan shows NONE and "sh run" does not show any member-vlan.	
Feature:	Topology Group	Function: VLAN Members
Service Request ID:	1194375	
Reported In Release:	NI 05.0.00	Probability: Medium

Defect ID:	DEFECT000471366	Technical Severity: Medium
Summary:	Diag burn-in on MP detects two kinds of failure	
Symptom:	Diag burn-in on MP detects two kinds of failure. Issue 1) "hwPhyPortRegRead() read valid bit timeout 88E1145 PHY - Failed" Issue 2) "Port 13 passed Port 14 failed Port 15 passed Port 16 passed Port 17 passed Port 18 passed Port 19 passed Port 23 passed Dx246 Switch Port Loopback - Failed"	
Feature:	System - XMR/MLX	Function: Diagnostics
Service Request ID:	1210187	
Reported In Release:	NI 05.3.00	Probability: Low

Defect ID:	DEFECT000471475	Technical Severity: Medium
Summary:	CER/CES may hang or unexpectedly reload after the user password is changed.	
Symptom:	This happens in rare conditions and appears to be dependent on the particular password value.	
Feature:	Character I/O	Function: Character Handling
Service Request ID:	1212475	
Reported In Release:	NI 05.4.00	Probability: Low

Defect ID:	DEFECT000472968	Technical Severity: Medium
Summary:	Metro ring RHP packets are not forwarded until preforwarding timer expires	
Symptom:	After CES link flaps the MRP ring master secondary port does not go into blocking until CES port goes into forwarding, causing network instability.	
Feature:	L2 Protocol	Function: MRP1
Service Request ID:	1219415,1219422	
Reported In Release:	NI 05.4.00	Probability: High

Defect ID:	DEFECT000473019	Technical Severity: Medium
Summary:	After removing vlans from global config, ospf redistribution stops working.	
Feature:	OSPF	Function: Redistribution
Service Request ID:	1196686	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000473100	Technical Severity: Medium
Summary:	When a static route pointing to null0 with distance 255 is configured, then the same static route with lower admin distance is not getting installed.	
Symptom:	The route that is expected to be installed is not installed.	
Feature:	IPv4 Static Route	Function: PROTOCOL
Service Request ID:	1221790	
Reported In Release:	NI 05.4.00	Probability: Low

Defect ID:	DEFECT000473619	Technical Severity: Medium
Summary:	max metric not going to active state with on start-up wait for bgp when router id not configured explicitly	
Workaround:	configure routes id.	
Feature:	OSPFv3	Function: PROTOCOL
Reported In Release:	NI 05.6.00	Probability: Medium

Defect ID:	DEFECT000474303	Technical Severity: Medium
Summary:	The adjusted Maximum burst size for 1 Gbps - 10 Gbps should be 2,147,450,880 instead of the current 1,410,064,384	
Symptom:	The problem is when average rate gets configured from 1Gbps to 10Gbps in CES platform.	
Feature:	CES Rate Limiting	Function: Port Based
Service Request ID:	1226361	
Reported In Release:	NI 05.4.00	Probability: Medium

Defect ID:	DEFECT000474815	Technical Severity:	Medium																																																	
Summary:	BFD timer value for 150ms flap when system max mac value is configured for 2097152																																																			
Symptom:	With this max mac config, Min time will always be around ~158 ms. If we are using Time-sensitive protocol less than 155ms, they will flap																																																			

With system-max mac as 2097152																																																				
LP-1#xxx pro mac show																																																				
MAC Profiling Data Begin																																																				
<table><tr><td>Name</td><td>TotalTB</td><td>TotalMs</td><td>#ofCalls</td><td>MinUS</td><td>MaxUS</td><td>AvgUS</td></tr><tr><td>MAC_PROFILE_AGING</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MAC_PROFILE_FLUSH</td><td>79105735</td><td>3164</td><td>20</td><td>158005</td><td>158790</td><td>158211</td></tr><tr><td>MAC_PROFILE_LEARN</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MAC_PROFILE_ACTION_HANDLER</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MAC_PROFILE_INFO_MP</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MAC_PROFILE_FLUSH_MP</td><td>0</td><td></td><td></td><td></td><td></td><td></td></tr></table>				Name	TotalTB	TotalMs	#ofCalls	MinUS	MaxUS	AvgUS	MAC_PROFILE_AGING	0	0	0	0	0	0	MAC_PROFILE_FLUSH	79105735	3164	20	158005	158790	158211	MAC_PROFILE_LEARN	0	0	0	0	0	0	MAC_PROFILE_ACTION_HANDLER	0	0	0	0	0	0	MAC_PROFILE_INFO_MP	0	0	0	0	0	0	MAC_PROFILE_FLUSH_MP	0					
Name	TotalTB	TotalMs	#ofCalls	MinUS	MaxUS	AvgUS																																														
MAC_PROFILE_AGING	0	0	0	0	0	0																																														
MAC_PROFILE_FLUSH	79105735	3164	20	158005	158790	158211																																														
MAC_PROFILE_LEARN	0	0	0	0	0	0																																														
MAC_PROFILE_ACTION_HANDLER	0	0	0	0	0	0																																														
MAC_PROFILE_INFO_MP	0	0	0	0	0	0																																														
MAC_PROFILE_FLUSH_MP	0																																																			
Feature:	System - XMR/MLX	Function:	IPC/ITC																																																	
Reported In Release:	NI 05.6.00	Probability:	Low																																																	

Closed defects without code changes in R05.6.00

This section lists defects closed without code changes in Multi-Service IronWare R05.6.00.

Reported release indicates the product and release that the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

This list was generated on September 24, 2013.

Defect ID: DEFECT000416603	Technical Severity: High
Summary: L2 ACL based outbound rate limiting in VPLS instance may incorrectly rate limit other VLANs.	
Symptom: Packet loss in the VPLS VLANs where rate limiting is not applied, or is not hitting the rate limit.	
Reason Code: Not Applicable	Probability: Low
Feature: VPLS - XMR/MLX	Function: Data Plane
Reported In Release: NI 05.2.00	Service Request ID: 762203

Defect ID: DEFECT000446222	Technical Severity: High
Summary: Disabling L2 LAG on primary backbone device makes network unreachable	
Symptom: During Failover testing , customer disabling primary port on 1/3L2 dynamic LAG in the primary MLX32 device of backbone, but it didnt recover the network thorough the secondary backbone router, Until customer enabled interface 1/3(Primary port og LAG) again. Below are the details.	
<p>Test Case 3 – Fail L2 LAG</p> <p>From kubmlx32-sfd2, disable port 1/3</p> <p>Target1 = 10.222.40.202 on port 4/3</p> <p>Target2 = 10.221.34.206 on port 2/3</p> <p>Target2 = 10.221.108.118 on port 24/1</p> <p>kubmlx32-sfd2</p> <p>-----</p> <p>lag "L2-kubmlx32-sfd1" dynamic id 14</p> <p>ports ethernet 1/3 ethernet 17/3</p> <p>primary-port 1/3</p> <p>deploy</p> <p>kubmlx32-sfd2(config-e1/3)#disable</p> <p>Ping output from PC:</p> <p>-----</p> <p>SSH@audmlx8-c1>TEST THREE</p> <p>Invalid input -> TEST THREE</p> <p>Type ? for a list</p> <p>SSH@audmlx8-c1>TEST THREE ping 10.221.34.206 count 150000 timeout 50 size 1000</p> <p>Sending 150000, 1000-byte ICMP Echo to 10.221.34.206, timeout 50 msec, TTL 64</p> <p>Request timed out.</p> <p>Request timed out.</p> <p>Request timed out.</p> <p>Request time</p>	
Reason Code: Not Reproducible	Probability: Medium
Feature: LAG - XMR/MLX	Function: Dynamic
Reported In Release: NI 05.2.00	Service Request ID: 1147831

Defect ID: DEFECT000450373	Technical Severity: High
Summary: SFM links briefly down on 2x100 at module boot or init time.	
Symptom: No known symptoms, appears to be cosmetic in nature.	
Workaround: Upgrade to 5200g or higher, where the issue is not seen.	
Reason Code: Already Fixed in Release	Probability: Medium
Feature: System - XMR/MLX	Function: SFM
Reported In Release: NI 05.2.00	Service Request ID: 1145847

Defect ID: DEFECT000461920	Technical Severity: High
Summary: Management switch-over followed by unexpected reboot.	
Reason Code: Not Applicable	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000464764	Technical Severity: High
Summary: External OSPF LSA database entry is present for a non-existent IP route.	
Symptom: The affected OSPF external LSA is getting propagated to other OSPF neighbors.	
Reason Code: Not Reproducible	
Feature: OSPF	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1192081

Defect ID: DEFECT000465703	Technical Severity: High
Summary: The device unexpectedly reloading in "bgp_RIB_out_delete_NLRI".	
Reason Code: Will Not Fix	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000468622	Technical Severity: High
Summary: Port is tied to non-existing VPLS id.	
Reason Code: Not Reproducible	
Feature: CES VPLS	Function: Forwarding
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000471220	Technical Severity: High
Summary: High CPU and 'Unexpected error: mcast set any AFI incorrect (35)' messages seen on console	
Reason Code: Not Applicable	
Feature: IPv4-MC PIM-DM Routing	Function: Forwarding - CES/CER
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000406159	Technical Severity: Medium
Summary: ip ospf database-filter may not work when it is configured on more than two VEs.	
Reason Code: Not Reproducible	
Feature: OSPF	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 742311

Defect ID: DEFECT000427206	Technical Severity: Medium
Summary: Slow memory failure on CES platform after upgrading to NI 5.2.0.0e.	
Symptom: Unable to ssh to the box – shows error message on console.	
Reason Code: Not Reproducible	Probability: Medium
Feature: SSHv2	Function: System Integration
Reported In Release: NI 05.2.00	Service Request ID: 1101625

Defect ID: DEFECT000427233	Technical Severity: Medium
Summary: PBIF issues with 5.4.0.0a code	
Reason Code: Not Reproducible	
Feature: FPGA	Function: PBIF
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000428044	Technical Severity: Medium
Summary: CPU MIB causes CPU to spike incrementally, sometimes even upto 2500%.	
Symptom: No impact to functionality.	
Reason Code: Already Fixed in Release	Probability: Medium
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.3.00	Service Request ID: 1085140

Defect ID: DEFECT000429791	Technical Severity: Medium
Summary: After LP move VPLS DA MAC is not programmed to CAM	
Symptom: High LP CPU after the move of a module from slot 14 to slot 11.	
<p>Debug packet capture shows that there is one particular flow that is forward in software.</p> <p>*****</p> <p>[ppcr_tx_packet] ACTION: Drop packet(reason: Unknown cause)</p> <p>[ppcr_rx_packet]: Packet received</p> <p>Time stamp : 01 day(s) 08h 48m 59s.,</p> <p>TM Header: [8013 b005 4000]</p> <p>Type: Fabric Unicast(0x00000008) Size: 78 Parity: 3 Src IF: 0</p> <p>Src Fap: 21 Dest Port: 0 Src Type: 0 Class: 0x00000000</p> <p>*****</p> <p>Packet size: 72, XPP reason code: 0x00008dd5</p> <p>00: 06f0 0003 1450 00d8-788b 8b04 0000 0000 FID = 0x06f0</p> <p>10: 0022 83fd 3829 001f-12be 05cf 0800 4500 Offset = 0x10</p> <p>20: 0028 62c6 4000 7a06-0d33 c147 6cd1 4137 VLAN = 216(0x00d8)</p> <p>30: 2187 08b6 01bb 2895-c80d f8f2 9fd1 5010 CAM = 0x5c582(L)</p> <p>40: 8000 0bd9 0000 0000-0000 8016 1005 8016 SFLOW = 0</p> <p>50: 1005 8016 1005 8016-1005 3d22 3235 223e DBL</p>	
Reason Code: Not Reproducible	Probability: Medium
Feature: VPLS - XMR/MLX	Function: Data Plane
Reported In Release: NI 05.3.00	Service Request ID: 1106508

Defect ID: DEFECT000434661	Technical Severity: Medium
Summary: MAC ACL put the LAG into LACP-BLOCKED state	
Symptom: MAC ACL on multiple LAG's and each LAG behaves differently.	
Workaround: Change the ACL: sh acc all be HIGH mac access-list XXX permit 0012.f2c2.1d00 ffff.ffff.ffff any 215 etype any permit 0012.f2c2.1d00 ffff.ffff.ffff any 216 etype any permit 0180.c200.0002 ffff.ffff.ffff any 4095 etype any permit 0012.f2c2.1dc1 ffff.ffff.ffff any 4095 etype any permit 0012.f2c2.1d93 ffff.ffff.ffff any 4095 etype any permit 0012.f2c2.1d93 ffff.ffff.ffff any any etype any permit 0012.f2c2.1dc1 ffff.ffff.ffff any any etype any deny any any any etype any log	
Reason Code: Not Reproducible	Probability: Medium
Feature: ACL - XMR/MLX	Function: L2 ACL
Reported In Release: NI 05.3.00	Service Request ID: 1116288

Defect ID: DEFECT000436745	Technical Severity: Medium
Summary: After an upgrade to 5200ch, root port is toggling between configured primary port and active primary port.	
Reason Code: Not Reproducible	Probability: Medium
Feature: L2 Protocol	Function: PVST
Reported In Release: NI 05.2.00	Service Request ID: 1127169

Defect ID: DEFECT000439246	Technical Severity: Medium
Summary: Command "show Lag brief" shows accumulated count of 10Gand 100G LAGs.	
Symptom: The output shows incorrect number of normal LAG and doesn't show the 100 LAG counts.	
Reason Code: Already Fixed in Release	Probability: Medium
Feature: LAG - XMR/MLX	Function: Static
Reported In Release: NI 05.3.00	Service Request ID: 1130545

Defect ID: DEFECT000441088	Technical Severity: Medium
Summary: Increase the maximum number of IPv6 Access Lists that can be configured on the MLX box.	
Reason Code: Not Applicable	
Feature: IPV6	Function: CONFIGURATION
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000441805	Technical Severity: Medium
Summary: TM log "Slot 1 PPCR 1 TM Reg offset 0x00003801" is generated frequently	
Symptom: tm log Feb 2 15:04:20: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00002600 Feb 2 15:04:19: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00002000 Feb 2 15:04:18: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00002000 Feb 2 15:04:13: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00000480 Feb 2 15:04:09: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00000400 Feb 2 15:04:00: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00000400 Feb 2 15:03:58: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00000600 Feb 2 15:03:54: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00002600 Feb 2 15:03:52: Slot 1 PPCR 1 TM Reg offset 0x00003801 Value 0x00002000	
Reason Code: Already Fixed in Release	Probability: Medium
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1132160

Defect ID: DEFECT000443807	Technical Severity: Medium
Summary: Connectivity issue noticed on 02/10	
Reason Code: Not Reproducible	Probability: Medium
Feature: IPv4 Forwarding - XMR/MLX	Function: Option HW Forwarding
Reported In Release: NI 05.1.00	Service Request ID: 1138178

Defect ID: DEFECT000443951	Technical Severity: Medium
Summary: Transparent hardware flooding causes NP packet drops in telemetry setup	
Reason Code: Not Reproducible	
Feature: Telemetry - XMR/MLX	Function: rule name
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000450312	Technical Severity: Medium
Summary: Not able to prepend Confederation As via Route map	
Reason Code: Not Applicable	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000451145	Technical Severity: Medium
Summary: latency when tcp window size increased on untag to tagged layer-3 flow	
Symptom: Latency increased on flows going from a tagged to untagged port and vice-versa when tcp parameters set to certain values.	
Reason Code: Can Not Fix	Probability: Medium
Feature: CES IPv4 Forwarding	Function: Routing
Reported In Release: NI 05.2.00	Service Request ID: 1132422

Defect ID: DEFECT000451841	Technical Severity: Medium
Summary: Using the VLAN keyword in an ACL in conjunction with a TCP or UDP range keyword, does not retain the VLAN keyword.	
Reason Code: Already Fixed in Release	
Feature: Telemetry - XMR/MLX	Function: ACL with vlan-id
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000452072	Technical Severity: Medium
Summary: Sflow sampling samples outbound traffic if the port is monitored.	
Reason Code: Will Not Fix	
Feature: CES SFLOW	Function: IPv4
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000452841	Technical Severity: Medium
Summary: When a new port is added to a vlan, packets are not forwarded by the PBR policy configured on the ve interface.	
Symptom: Packets matching PBR configuration were not being forwarded to firewall.	
Workaround: Use 'ip rebind-acl all' command to clear condition.	
Reason Code: Not Reproducible	Probability: Medium
Feature: PBR - XMR/MLX	Function: IPv4
Reported In Release: NI 05.2.00	Service Request ID: 1158050

Defect ID: DEFECT000453150	Technical Severity: Medium
Summary: 3 out of 32 port LAG show less than 1% utilization in MLX. Other Lag ports are showing 40% utilization.	
Symptom: No other issues observed on other ports.	
Workaround: Bouncing the Primary LAG ports will resolve the issue.	
Reason Code: Not Applicable	Probability: Medium
Feature: LAG - XMR/MLX	Function: Dynamic
Reported In Release: NI 05.2.00	Service Request ID: 1162315

Defect ID: DEFECT000454183	Technical Severity: Medium
Summary: Auto upgrade feature fails to upgrade an FPGA image on a newly inserted module.	
Symptom: Received the following error when copying the FPGA image via TFTP: "Error:LP Upgrade: invalid XPP FPGA card type 1".	
Reason Code: Not Applicable	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Reported In Release: NI 05.3.00	Service Request ID: 1161752

Defect ID: DEFECT000454252	Technical Severity: Medium
Summary: 24x1 card experienced an unexpected reset with CAM IPVPN partition warning.	
Reason Code: Will Not Fix	
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000455270	Technical Severity: Medium
Summary: In an L3VPN configuration the management module unexpectedly reloaded.	
Reason Code: Not Applicable	
Feature: Inter-VRF-Routing	Function: CONFIGURATION
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000456866	Technical Severity: Medium
Summary: Slot 15 (8x10) report high Latency	
Reason Code: Already Fixed in Release	
Feature: TM/SFM	Function: Forwarding - Multicast Traffic
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000457309	Technical Severity: Medium
Summary: MSDP peering did not re-establish after a system reboot.	
Symptom: MSDP was down after the reboot and had to be reconfigured before it would come up.	
Reason Code: Not Reproducible	Probability: High
Feature: IPv4-MC MSDP	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1106026

Defect ID: DEFECT000457332	Technical Severity: Medium
Summary: L4 rule-based CAM entry may not be released via SNMP SET(TFTP config download = snAgCfgLoad brcdIp.1.1.2.1.9).	
Reason Code: Already Fixed in Release	
Feature: SNMP Management	Function: Layer4 ACL-RL Mib
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000458515	Technical Severity: Medium
Summary: With vll-local configuration seeing unicast streams drops.	
Symptom: Seeing unicast VOD streams drop when there is a parallel lag connection for multicast streams.	
Reason Code: Not Reproducible	
Feature: CES VLL	Function: Local
Reported In Release: NI 05.0.00	Service Request ID: 1167255

Defect ID: DEFECT000458790	Technical Severity: Medium
Summary: MLX advertised prohibited routes to the neighbors.	
Symptom: Prohibited routes advertised by the router.	
Reason Code: Not Reproducible	Probability: Low
Feature: BGP	Function: BGPv4
Reported In Release: NI 05.2.00	Service Request ID: 1170664

Defect ID: DEFECT000459892	Technical Severity: Medium
Summary: Flow Statistic on controller is not working.	
Reason Code: Not Reproducible	
Feature: Openflow Extender	Function: Extender-Configuration
Reported In Release: NI 05.4.00	

Defect ID: DEFECT000461559	Technical Severity: Medium
Summary: Only on systems running NI 5.2.00j, routes with no-export community are being announced to eBGP peers. NI 5.2.00j was the only released version containing this issue.	
Symptom: Routes with well-known communities are not being processed correctly, and may be incorrectly announced to other BGP peers, if an inbound route-map was used to modify the received BGP attributes. This occurs only on systems running NI 5.2.00j.	
Workaround: Use a route-map to filter out routes with a "no-export" community value. <p>The route-map filtering can filter any BGP community values, including the well-known community attributes.</p> <p>The following example shows how to filter out routes with the "no-export" community value:</p> <pre>ip community-list no-export-community-acl seq 5 permit no-export route-map customer-filter deny 1 match community no-export-community-acl route-map customer-filter permit 5</pre>	
Reason Code: Not Applicable	Probability: High
Feature: BGP	Function: BGPv4
Reported In Release: NI 05.2.00	Service Request ID: 1186974

Defect ID: DEFECT000462382	Technical Severity: Medium
Summary: acl-duplication-check restricts configuring permit/deny icmp any any 1/2/3	
Symptom: If "permit icmp any any 1" is configured, "permit icmp any any 2" statement cannot be configured.	
Reason Code: Already Fixed in Release	
Feature: ACL - XMR/MLX	Function: IPv6 ACL
Reported In Release: NI 05.5.00	Service Request ID: 1172392

Defect ID: DEFECT000463784	Technical Severity: Medium
Summary: Diag burn-in on a CES 2048CX running NI 5.4.00c fails intermittently.	
Reason Code: Not Reproducible	
Feature: Chassis/Hw Management	Function: Diagnostics (burn-in)
Reported In Release: NI 05.4.00	

Closed defects with code changes in R05.6.00

This section lists defects closed with code changes in Multi-Service IronWare R05.6.00. Note that when a workaround to an issue is available, it is provided.

Reported release indicates the product and release in which the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

This list was closed on September 24, 2013.

Defect ID: DEFECT000414410	Technical Severity: High
Summary: In a large OSPFv3 LSA environment, an LS update was retransmitted before the re-transmission interval expired.	
Symptom: The LS update was re-transmitted and the message "OSPFv3: Intf retransmit" appeared every 30 minutes.	
Feature: OSPFv3	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 753073

Defect ID: DEFECT000422796	Technical Severity: Critical
Summary: In rare cases of reload the SPAUI link between TM and XPP goes Down resulting in LACP to go in LACP-BLOCKED state	
Symptom: LAG is two link LAG between JNPR (R24) and BRCD (R32). JNPR stats show Tx & Rx as expected and mirroring inbound traffic on R32 shows lacp packets received from JNPR as expected every second. R32 LP debugs shows no lacp packets received. NO NP or TM drops are observed.	
Feature: FPGA	Function: XPP-8x10
Reported In Release: NI 05.4.00	Service Request ID: ,1201023

Defect ID: DEFECT000425483	Technical Severity: High
Summary: A BGP neighbor outbound route update seems slow when updating/bringing up one peer in a large peer-group configuration.	
Symptom: The slowness is compared to the same operation on a smaller peer group configuration.	
Feature: BGP	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1090132

Defect ID: DEFECT000426116	Technical Severity: Medium
Summary: Experiencing multicast packet loss when forwarding from 1G to 10G interfaces.	
Symptom: Multicast traffic and CCM packets that transit CER/CES are intermittently dropped.	
Workaround: Put VPLS ports and MC port on the same Packet processor (port group).	
Feature: CES 802.1ag	Function: VPLS
Probability: Low	
Reported In Release: NI 05.1.00	Service Request ID: 1088924,1088924

Defect ID: DEFECT000431482	Technical Severity: Medium
Summary: Power-off 8x10 result in 2x100 OSPF link to get stuck in EXSTART/EXCHANGE state	
Feature: System - XMR/MLX	Function: SFM
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1085907

Defect ID: DEFECT000431900	Technical Severity: Medium
Summary: An ARP request from a particular source MAC failed to transmit between a pair of MLXs with a LAG configured between them.	
Symptom: In a very rare case, the ARP request for a particular MAC address did not get transmitted across the LAG.	
Workaround: Disable the affected LAG port that is the current Active Lead port, seen in 'sh lag'.	
Feature: L2 Forwarding - XMR/MLX	Function: MAC
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1109407

Defect ID: DEFECT000435843	Technical Severity: Critical
Summary: Under certain traffic pattern conditions with varying packet sizes, the data portion of the packet may be corrupted when traversing the 100G module.	
Symptom: After particular files are transferred, the checksum is incorrect. When this is observed, the traffic most often is characterized by jumbo packet sizes or non-jumbo packets at a very high traffic rate.	
Feature: IPv4 Forwarding - XMR/MLX	Function: MTU
Reported In Release: NI 05.4.00	Service Request ID: 1120693

Defect ID: DEFECT000436697	Technical Severity: High
Summary: In a specific situation, sending an edit-config RPC for MPLS using NetConf may lead to service interruption.	
Symptom: Reordering the RSVP and LSP containers in an RPC sent to a NetIron device may lead to a service interruption when debug output is redirected to a second SSH session and the LSP is being enabled in the RPC.	
Workaround: Reorder the mpls-config sub containers in the following order: path, lsp, rsvp.	
Feature: NetConf	Function: SSH Layer
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1126807,1126807

Defect ID: DEFECT000436705	Technical Severity: High
Summary: Using NetConf, the RSVP container exits before execution of the container leafs.	
Symptom: An edit-config RPC for mpls-config with an RSVP container does not execute.	
Workaround: Configure RSVP parameters using the normal CLI.	
Feature: NetConf	Function: Engine
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1126807

Defect ID: DEFECT000437901	Technical Severity: High
Summary: BGP convergence slow with outbound route-map applied to many members of a peer-group.	
Symptom: Route convergence slow outbound when peer-group contains many peers sharing the same route-map.	
Feature: BGP	Function: BGPv4
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1087001

Defect ID: DEFECT000438196	Technical Severity: Medium
Summary: QOS not marking CFM packets properly.	
Symptom: CFM packets may not be given the appropriate QOS value, based on the configuration.	
Feature: MPLS OAM	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1130330

Defect ID: DEFECT000438276	Technical Severity: Medium
Summary: In a rare situation a 4x10G module unexpectedly reloaded after adding a new VPLS instance to the configuration.	
Symptom: The service on the module will be interrupted for 1-2 minutes while the module reloads.	
Feature: MPLS	Function: Application API
Probability: High	
Reported In Release: NI 05.2.00	Service Request ID: 1131434

Defect ID: DEFECT000441972	Technical Severity: Medium
Summary: PIM Pruning Multicast stream although IGMP joins are still active but MLX timeout with KAT timer expired.	
Feature: IPv4-MC IGMP	Function: IGMPv3 Protocol
Reported In Release: NI 05.4.00	Service Request ID: 1121573

Defect ID: DEFECT000442150	Technical Severity: Medium
Summary: 100G port flaps randomly at least once every day.	
Symptom: Random port flaps: Jan 31 23:32:37:I:System: Interface ethernet 1/2, state up Jan 31 23:32:36:I:System: port 1/2 is down(remote fault)	
Feature: System - XMR/MLX	Function: Link Fault Signaling
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1136028

Defect ID: DEFECT000442736	Technical Severity: Medium
Summary: The SNMP command 'snmpbulkwalk' is not using the outbound interface MTU.	
Symptom: snmpbulkwalk is using the global MTU setting, instead of the setting for the specific outbound interface MTU.	
Feature: IPv4	Function: UDP
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1138148

Defect ID: DEFECT000443139	Technical Severity: High
Summary: OSPF flap on 100G module insertion	
Symptom: After 2x100G module was inserted in slot 27, OSPF adjecencies on LP9 and LP21 unexpectedly flapped.	
Feature: OSPF	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1115968

Defect ID: DEFECT000443576	Technical Severity: Medium
Summary: Management module may unexpectedly reload while processing an RSVP-TE session.	
Symptom: If the system has dual management modules, the system will experience a switchover. If a single Management module is installed, then there will be service impact for about 3 minutes while the system reloads.	
Feature: MPLS Forwarding - XMR/MLX	Function: MPLS over VE
Probability: High	
Reported In Release: NI 05.3.00	Service Request ID: 1141311

Defect ID: DEFECT000443905	Technical Severity: Medium
Summary: New Gen2 8x10G module: tower 2 TM not forwarding traffic.	
Symptom: For a particular Gen2 8x10G module, tower 2 TM ports are not able to learn ARP, so the traffic is not forwarded.	
Feature: TM/SFM	Function: Health monitoring
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1131599

Defect ID: DEFECT000444897	Technical Severity: Medium
Summary: In a rare case, an IPv6 forwarding problem occurs when the timing of a hardware addition was assessed incorrectly as a drop.	
Symptom: Connectivity issue seen with an IPv6 flow.	
Feature: IPv6 Forwarding - XMR/MLX	Function: Hardware Forward
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1144686

Defect ID: DEFECT000445099	Technical Severity: High
Summary: An interface module may have an unexpected reload processing an IPv6 ND when IPv6 neighbors reach the maximum allowable number.	
Symptom: The interface module will be impacted for 1 minute while the card reloads.	
Workaround: Upgrade to NI 05.4.00 code, where scaling for IPv6 ND is at 32k.	
Feature: IPV6	Function: Neighbor Discovery
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1145884

Defect ID: DEFECT000445526	Technical Severity: Medium
Summary: RSVP messages are sent on a less preferred route only (e.g., a default route), after deleting and adding the more specific route (e.g., /30).	
Symptom: PATH msg is forwarded to the less specific route's next-hop. If an RSVP destination is reachable via default route (0.0.0.0/0), it will not switch to use a better (more specific) route when a better route becomes available in RTM. This causes PATH msgs to get forwarded to the incorrect hop. The incorrect hop, upon receiving the PATH msg, will generate a PATH Error with "routing error", "top hop not it's local address" error. As a result, the LSP will not come up. Note that this issue is only applicable if RSVP is using a default route. Non default routes do not have this issue.	
Feature: RSVP-TE	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1145613

Defect ID: DEFECT000445590	Technical Severity: Medium
Summary: MCT KeepAlive control packet is not being forwarded if CER & MLX devices act as a pass-through.	
Symptom: The MCT KeepAlive control packet is dropped when the pass-through device is not configured with MCT.	
Feature: MCT	Function: CES_L2_FWD
Probability: Low	
Reported In Release: NI 05.2.00	Service Request ID: 1130330

Defect ID: DEFECT000445872	Technical Severity: Medium
Summary: GRE Interface status from SNMP polling shows incorrect information for a disabled GRE tunnel interface.	
Symptom: Status is displayed as Up/Down, when the tunnel status is Down/Down.	
Feature: SNMP Management	Function: System Management Mib
Probability: High	
Reported In Release: NI 05.1.00	Service Request ID: 1137258

Defect ID: DEFECT000446451	Technical Severity: Medium
Summary: MLX not responding to LBM frames on local VPLS.	
Symptom: During OAM testing, the MLX is not responding to LBM frames on a local VPLS. It works properly if sent to a remote MEP.	
Workaround: If the down MEP is created on the connected port, it will work as expected. If it cannot be created on the connected port, the up MEP should be configured on the remote VPLS peer.	
Feature: PBB-OAM	Function: ESI
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: Case Number 1146909

Defect ID: DEFECT000446703	Technical Severity: Medium
Summary: 100G-CFP-10x10 optical modules may experience a random reset, causing a 1 second link flap.	
Symptom: The frequency between resets is typically days. When a CFP resets due to this issue, both sides of the link will report a link DOWN and a link UP event within a 1 second time stamp (i.e., link flap). It may or may not be accompanied by a Remote or Local Fault alarm, depending on the LFS setting and the type of transport equipment, if any, in-between. The link down/up status is available through the System Log and SNMP. Note that a link flap can be triggered by other reasons, such as an optical fiber cable issue, a transport equipment issue, or other faults.	
Workaround: This workaround should be performed during a maintenance window. The workaround will cause the link to go down and come back up. The workaround involves reading and writing registers to execute a sequence of initialization steps to put the CFP into the correct operational mode. In order for the workaround to be effective, the sequence must be run via a script so the timing between steps is well controlled. Remote access to the line card is required to execute the workaround. Brocade has a script available written for Tera Term version 4.7. Tera Term is a free open source terminal emulator available to the public. Please contact Brocade Support to coordinate a time to schedule a maintenance window and remote access to implement the workaround. After the terminal emulator is set up, the script takes approximately ten seconds per port to execute, and the actual down time on each port is approximately one second.	
Feature: MAC/Phy	Function: Link Status
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1148372,1149707

Defect ID: DEFECT000446756	Technical Severity: Medium
Summary: IPv4 and IPv6 route-maps with multiple "set next-hop" statements fail to acknowledge loss or recovery of the first next-hop when port ranges are used in the match condition ACL.	
Symptom: Packets are dropped instead of forwarded to a secondary next hop when a route-map's first configured next hop becomes unreachable.	
Workaround: For a temporary workaround, delete the "ip policy" or "ipv6 policy" config line from its interface then re-add it. This will last until the next time the reachability of the first next-hop changes. For a more permanent workaround, in IPv4 and IPv6 PBR route map match ACLs, never use port ranges and always use specific ports.	
Feature: PBR - XMR/MLX	Function: IPV6
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1148545

Defect ID: DEFECT000447468	Technical Severity: Medium
Summary: Logging low RX power alarms/warnings when LOS is asserted (port is down).	
Symptom: 4x10G module with optical monitoring enabled for default of 3 minutes is logging alarms for a period of seconds. When the value is changed to 5 minutes, it is logging the alarm per the configured interval but it is restricted to only one port (logging alarm for port 1/1 alone). No logs for the other ports (1/2-1/4) though it has low alarm in "show optic 1" outputs.	
Feature: System - XMR/MLX	Function: Ethernet Optics
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1085737

Defect ID: DEFECT000448126	Technical Severity: Medium
Summary: By removing "CDP" and "FDP" from the config, "no cdp enable" and "no fdp enable" stayed in the config of VPLS end points, which cannot be removed.	
Symptom: CDP and FDP cannot be removed from the VPLS endpoints. If CDP and FDP are removed from the global config, the ports cannot be added in the LAG.	
Feature: FDP-CDP	Function: CLI
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1150164

Defect ID: DEFECT000448514	Technical Severity: Medium
Summary: In rare cases, the standby management module unexpectedly reloaded while processing licensing functionality with 2x100G module present.	
Symptom: In rare cases, the standby module was reloaded when the configuration was copied via SCP to a PCMCIA card and then copied to the running-config and a write mem executed. The unexpected reload happened when the Update License timer expired after the above config changes were applied.	
Workaround: The standby management module will reload and come back up without any impact to the existing traffic or functionality.	
Feature: SNMP Management	Function: Engine
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1151046

Defect ID: DEFECT000448774	Technical Severity: Medium
Summary: Inter VRF forwarding problem on a CES device.	
Symptom: Directly connected host on one VRF cannot reach another VRF.	
Feature: CES IPv4 Forwarding	Function: VRF-lite
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1143088

Defect ID: DEFECT000449925	Technical Severity: High
Summary: Client-interface shutdown does not keep all CCEP ports in disabled state after MCT node reload	
Symptom: After upgrading from 5.3 to 5.5, client-interfaces shutdown command was configured and then the device was reloaded. After the node came up, not all CCEP ports are in disabled state even though the running-config has the command in the cluster config.	
Workaround: Increase client-int delay to 120 sec or more.	
Feature: MCT-L2VPN	Function: Infrastructure
Probability: High	
Reported In Release: NI 05.5.00	Service Request ID: 1212893

Defect ID: DEFECT000449954	Technical Severity: Medium
Summary: TACACS+authorization commands which are not allowed to be run are able to be executed by a user if they are in an ACL editing context	
Symptom: Any commands made in ACL edit mode are not properly authenticated.	
Feature: AAA	Function: TACACS+ Authorization
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153064

Defect ID: DEFECT000449995	Technical Severity: Medium
Summary: MIB counter for "GoodOctets" is incorrect.	
Symptom: Command regarding MIB counter is giving a negative value for "GoodOctets" for both RX and TX.	
Feature: UNDETERMINED	Function: UNDER REVIEW
Probability: Low	
Reported In Release: NI 05.3.00	Service Request ID: 1151090

Defect ID: DEFECT000450126	Technical Severity: High
Summary: LSP is torn down when a port for secondary FRR path goes down.	
Symptom: May receive log messages that the LSP Primary path went down.	
Feature: MPLS Control Plane	Function: LSP Manager
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1143968

Defect ID: DEFECT000450434	Technical Severity: High
Summary: 2x100G module throughput is not 100% on an MLX chassis.	
Symptom: When 100G traffic is sent through a 2x100G module, the OutUtilization is only ~63G in NORMAL mode and ~73% in TURBO mode.	
Feature: TM/SFM	Function: Performance (Throughput Latency)
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000451026	Technical Severity: Medium
Summary: In MCT over VPLS network some hosts can communicate while others cannot.	
Symptom: MCT over VPLS on the network and a few hosts cannot communicate across VPLS.	
Feature: MCT-VPLS	Function: CES-Hw Forwarding
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1155797,1152119

Defect ID: DEFECT000451642	Technical Severity: Medium
Summary: SSH users not timing out at configured "ip ssh idle-time".	
Symptom: SSH users are not timing-out after the configured ssh idle-timeout has expired. Example: ip ssh idle-time 15 SSH connections (inbound): 1 established, client ip address x.x.x.x, user is ssh1, privilege super-user using vrf default-vrf. 37 minutes 11 seconds in idle	
Feature: SSHv2	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1105020

Defect ID: DEFECT000451688	Technical Severity: Medium
Summary: After upgrading an MLXe-32 to NI 05.4.00b, SFM links go down and TM errors are seen.	
Symptom: SFM link disabled by system health monitor errors.	
Feature: TM/SFM	Function: Health monitoring
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1157797, 1132160

Defect ID: DEFECT000451855	Technical Severity: Medium
Summary: Multicast traffic loss may occur when an unrelated module is powered-off.	
Symptom: Multicast traffic loss is observed when an LP is powered off and that LP is not in the data path of the source and receiver.	
Feature: TM/SFM	Function: Forwarding - Multicast Traffic
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1157186

Defect ID: DEFECT000451898	Technical Severity: Medium
Summary: The "snAgSysLogGblCriticalLevel.0" OID (.1.3.6.1.4.1.1991.1.1.2.6.1.4.0) cannot be set to a value greater than 128.	
Symptom: The snChasWarningTemperature MIB does not read any values. The snAgSysLogGblCriticalLevel MIB cannot be set to a value greater than 128.	
Feature: SNMP Management	Function: System Management Mib
Reported In Release: NI 05.3.00	Service Request ID: 1157399

Defect ID: DEFECT000452455	Technical Severity: Medium
Summary: Port LED stays green when a CER/CES port configured "gig-default neg-off" is disabled using the CLI.	
Symptom: When a 1G interface with "gig-def neg-off" configured is disabled using the CLI, the port LED on the front panel stays green, even though the port is Down.	
Feature: CES SYSTEM	Function: PHY
Reported In Release: NI 05.4.00	Service Request ID: 1158705

Defect ID: DEFECT000452630	Technical Severity: Medium
Summary: When using the 'debug packet capture' command, the CER/CES does not strip the tag and sends a tagged packet on an untagged port configured as dual mode.	
Symptom: Unexpected result seen on the dual mode untagged port.	
Workaround: Run the command "no debug packet capture."	
Feature: L2 Forwarding - XMR/MLX	Function: Forwarding
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1158895

Defect ID: DEFECT000453085	Technical Severity: Medium
Summary: ACL is not working on port 7/1 and 7/4 but the same ACL is filtering traffic on 7/2 and 7/3.	
Symptom: ACL is not filtering traffic on port 7/1 and 7/4, which can cause security hole.	
Workaround: --	
Feature: ACL - XMR/MLX	Function: ACL policy
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1159069

Defect ID: DEFECT000453388	Technical Severity: Medium
Summary: CER/CES platform sends incorrect trap when the power supply unit is pulled from the chassis.	
Symptom: CER/CES sends snTrapChasPwrSupplyOK trap when the power supply unit is pulled from the chassis.	
Feature: SNMP Management	Function: Trap/Notification
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1155396

Defect ID: DEFECT000453549	Technical Severity: Medium
Summary: MLX may unexpectedly reload when shutting down a peer-group with more than 100 neighbors with 400K outbound routes for each neighbor.	
Symptom: The device was reloaded when the user shut down a peer group.	
Feature: BGP	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1162827

Defect ID: DEFECT000453772	Technical Severity: Medium
Summary: Standby management module may reload while copying the config to the PCMCIA card.	
Symptom: There is no service impact when a standby management module reloads.	
Feature: System - XMR/MLX	Function: Image/FPGA copy
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1152758

Defect ID: DEFECT000453909	Technical Severity: High
Summary: Link keepalive configuration might not be parsed when upgrading from NI 5.2.00e to 5.3.00e if ports are part of a LAG.	
Symptom: When upgrading the device from NI 5.2.00e to 5.3.00e, some link-keepalive lines were not parsed causing the ports to stay down in the peers; and some devices were not working after the upgrade.	
Workaround: To recover, re-add the link-keepalive configuration for the missing ports.	
Feature: UDLD	Function: CLI
Probability: High	
Reported In Release: NI 05.3.00	Service Request ID: 1162695

Defect ID: DEFECT000453930	Technical Severity: Medium
Summary: When a port is removed from the LAG configuration, then the output of 'show vlan eth slot/port' shows the port is a member of configured VLANs on the system.	
Symptom: Shows incorrect information about the configured VLANs on the port.	
Feature: LAG - XMR/MLX	Function: Static
Reported In Release: NI 05.4.00	Service Request ID: 1165101

Defect ID: DEFECT000453941	Technical Severity: Medium
Summary: Provide information in show version' output that will indicate whether 1 port or 2 ports can be used (for 100G LP).	
Symptom: From the output of show version, it cannot be determined whether the module has 1 port or 2 port license.	
Feature: CLI Infrastructure	Function: Real Time Monitoring
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1135911

Defect ID: DEFECT000454040	Technical Severity: High
Summary: A 2x100 module will not support 100% line rate throughput on an MLX chassis.	
Symptom: A 2x100 module TM will see drops when sending line-rate traffic.	
Feature: System - XMR/MLX	Function: TM
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000454209	Technical Severity: Medium
Summary: Static IGMP group entries are aging out when the global multicast age is changed from the default.	
Symptom: When the multicast age was at 30 seconds, the static entry aged out.	
Feature: IPv4-MC IGMP	Function: IGMP static entries
Reported In Release: NI 05.4.00	Service Request ID: 1166157

Defect ID: DEFECT000454381	Technical Severity: Medium
Summary: Broadcast packet of VPLS link is not transmitted from LAG port after switchover.	
Symptom: Broadcast packet of VPLS link is not transmitted from LAG port after ESS MCT primary switchover.	
Workaround: Disable/enable the LAG port.	
Feature: MPLS Forwarding - XMR/MLX	Function: MPLS over LAG
Probability: Medium	
Reported In Release: NI 05.3.00	Service Request ID: 1154483

Defect ID: DEFECT000454509	Technical Severity: Critical
Summary: When Auto-Tuning is enabled, multicast packets may be dropped during the time that tuning is in progress.	
Symptom: Multicast packet loss might occur on some line cards during the auto-tuning process.	
Feature: TM/SFM	Function: Auto-tuning
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1161174

Defect ID: DEFECT000454591	Technical Severity: High
Summary: OSPF Session is resetting due to too many retransmissions	
Symptom: OSPF Session will flap and cause network impact.	
Feature: OSPF	Function: L3 VPN
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1165356

Defect ID: DEFECT000454936	Technical Severity: Medium
Summary: Cannot ping from host to host thru VLL.	
Symptom: When bringing up a cross-connect over a VLL, the interfaces and the VLL would come up, but the traffic did not make the connection.	
Workaround: Clear the ARP entry of the MPLS next hop. This refreshes the NHT entry.	
Feature: CES VLL	Function: Forwarding
Reported In Release: NI 05.2.00	Service Request ID: 1165243

Defect ID: DEFECT000454945	Technical Severity: Medium
Summary: VLL end-points are not passing LACP PDUs with forward-lacp configured if route-only is enabled globally.	
Symptom: LACP is not coming up across VLL.	
Feature: VLL - XMR/MLX	Function: VLL
Reported In Release: NI 05.2.00	Service Request ID: 1163591 and 1167145

Defect ID: DEFECT000455043	Technical Severity: Medium
Summary: DMM reflection on a local VPLS with multiple CE VLANs is not working.	
Symptom: When sending a DMR to a local VPLS MEP, there is no response if there are multiple VLAN IDs.	
Feature: MPLS OAM	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1166191

Defect ID: DEFECT000455228	Technical Severity: Medium
Summary: CLI and SNMP report a different number of temperature sensors for the 24x10G module.	
Symptom: The number of temperature sensors reported by the CLI command "show chassis" for the 24x10G module is not consistent with that of the SNMP report.	
Workaround: Use the "show chassis" CLI command to see the active sensors on the module.	
Feature: SNMP Management	Function: Engine
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1127000

Defect ID: DEFECT000455298	Technical Severity: Medium
Summary: MAC movement in VRF is not detected correctly.	
Symptom: After moving the host from one port to another in the same VLAN, the host is not reachable by a device from another VRF.	
Feature: CES IPv4 Forwarding	Function: VRF-lite
Reported In Release: NI 05.4.00	Service Request ID: 1166625

Defect ID: DEFECT000455315	Technical Severity: High
Summary: Elevated CPU utilization only on the Management module for the mcast and ip_receive task, with no service interruption.	
Symptom: Management sessions may be slowed down.	
Feature: UNDETERMINED	Function: UNDER REVIEW
Reported In Release: NI 05.3.00	Service Request ID: 1166971

Defect ID: DEFECT000455478	Technical Severity: Medium
Summary: OSPF redistributed static routes disappear from OSPF neighbors.	
Symptom: OSPF routers stop receiving redistributed static routes from the neighbors.	
Feature: OSPF	Function: Redistribution
Reported In Release: NI 05.4.00	Service Request ID: 1161563 and 1169278

Defect ID: DEFECT000455612	Technical Severity: High
Summary: Unable to configure LDP-SYNC on Ethernet interface 1/1.	
Symptom: Unable to use the CLI to configure LDP Sync on Ethernet port 1/1.	
Workaround: Use port 1/1 as an untagged port in the VLAN and create a virtual interface. <pre> vlan 10 untagged ethe 1/1 router-interface ve 10 ! ! router ospf area 0 ldp-sync ! interface ve 10 ip ospf area 0 ip ospf network point-to-point ip ospf ldp-sync enable ip address xx.xx.xx.1/24 </pre>	
Feature: LDP	Function: LDP-IGP sync
Probability: Low	
Reported In Release: NI 05.4.00	Service Request ID: 1154130

Defect ID: DEFECT000455817	Technical Severity: High
Summary: The tag values are not matching correctly with the route-map in the OSPF VRF distribute list.	
Symptom: The distribute list will not work as expected.	
Workaround: Do not use route-map with distribute-list for OSPF filtering. Use distribute-list with standard access-list alone. This creates an access-list and denies the specific prefixes, permitting the remaining ones. Example: Standard IP access list 21 deny 10.1.0.0 0.0.xxx.xxx deny 10.2.0.0 0.0.xxx.xxx permit any <pre> router ospf vrf test1 area 110 redistribute connected redistribute static route-map redid_map1 log adjacency distribute-list 21 in </pre>	
Feature: VRF	Function: CLI
Reported In Release: NI 05.1.00	Service Request ID: 1168149

Defect ID: DEFECT000455905	Technical Severity: High
Summary: Packet checksum errors causing IPv6 communication issues.	
Symptom: IPv6 NS for anycast address may trigger corruption in the NA reply packet.	
Workaround: Do not use IPv6 anycast address.	
Feature: IPV6	Function: Neighbor Discovery
Reported In Release: NI 05.4.00	Service Request ID: 1164891

Defect ID: DEFECT000456020	Technical Severity: Medium
Summary: Modified ACLs using TFTP may not work correctly when the ACL is being deleted at the global level and reconfigured using TFTP.	
Symptom: ACLs may not be applied properly, causing unexpected behavior.	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.4.00	Service Request ID: 1168434

Defect ID: DEFECT000456162	Technical Severity: High
Summary: IP packet is not transmitted from VE port in accordance with IP routing table.	
Symptom: Issue experienced while using Ping functionality.	
Feature: IPv4 Forwarding - XMR/MLX	Function: FIB
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1168193,1179903

Defect ID: DEFECT000456449	Technical Severity: High
Summary: Control packets should be given higher CPU priority so that lower priority packets cannot impact the control plane.	
Symptom: BFD and control plane impact noted: attempt to initiate an SSH session failed and OSPF flaps were observed.	
Feature: BFD	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1154675,1154675

Defect ID: DEFECT000456509	Technical Severity: Medium
Summary: After a software upgrade, an MLX32 MLX device is misrepresented as an XMR in the FDP output.	
Symptom: After a software upgrade, an MLX-3200 is shown as an XMR-32000.	
Feature: FDP-CDP	Function: PROTOCOL
Probability: Medium	
Reported In Release: NI 05.2.00	Service Request ID: 1153498

Defect ID: DEFECT000456757	Technical Severity: Medium
Summary: When configuring the ipv6 ND reachable-time on an interface, "show ipv6 interface e <slot/port>" displays inconsistent output.	
Symptom: "show ipv6 interface e <slot/port>" displays ND reachable time incorrectly.	
Feature: IPV6	Function: Neighbor Discovery
Reported In Release: NI 05.4.00	Service Request ID: 1167966

Defect ID: DEFECT000456813	Technical Severity: Medium
Summary: LP 16 not forwarding traffic after MLXe-16 upgraded to 5.4.00bd	
Symptom: After upgrading router to 5.4.00bd ports on LP 16 were not forwarding traffic as expected.	
Workaround: Power cycle LP	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Probability: Medium	
Reported In Release: NI 05.4.00	Service Request ID: 1169705

Defect ID: DEFECT000456977	Technical Severity: Medium
Summary: SNMP poll of OID 1.3.6.1.2.1.2.2.1.21 - ifOutQLen shows abnormally high values.	
Symptom: The high values do not correspond to the port statistics.	
Feature: SNMP Management	Function: Layer2 Mib
Reported In Release: NI 05.3.00	Service Request ID: 1166574

Defect ID: DEFECT000457469	Technical Severity: Medium
Summary: After reload the L4 CAM may not get programmed from a PBR configuration on the ingress module, causing unexpected forwarding results.	
Symptom: After upgrade, traffic is not being forwarded on all ports. The issue is specific to heavily loaded systems, with a PBR configuration. Systems with no PBR config are not susceptible to this issue. The issue can also happen on the reload of the whole system.	
Workaround: Follow the steps below to recover from the condition: 1. Remove pbr config. 2. Power cycle the module. 3. Reapply pbr config.	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1169233,1169233,1169

Defect ID: DEFECT000457665	Technical Severity: Medium
Summary: The response from remote MEPs is getting delayed because packets are trapped to the CPU at an intermediate node.	
Symptom: The delay in the MEP response may cause a link to go down, which may be service impacting.	
Feature: 802.1ag over VPLS	Function: CCM - Sub-second Timer
Reported In Release: NI 05.3.00	Service Request ID: 1150554

Defect ID: DEFECT000458550	Technical Severity: Medium
Summary: On the CER, an access-list configured with dscp-marking followed by drop-precedence is not working.	
Symptom: The expected behavior for the ACL is not seen.	
Feature: CES ACL	Function: L2 ACL
Reported In Release: NI 05.5.00	Service Request ID: 1169814

Defect ID: DEFECT000458561	Technical Severity: Medium
Summary: In case PIM is disabled, MP resets when pim dr-priority is configured to an interface	
Symptom: MP may reset unexpectedly when pim dr-priority value is configured from CLI.	
Feature: PIM Multinet	Function: CLI
Reported In Release: NI 05.4.00	Service Request ID: 1172077

Defect ID: DEFECT000458791	Technical Severity: High
Summary: Unable to telnet when "ip telnet source-interface loopback 1" is configured.	
Symptom: Error message: "Inactive source address" is received.	
Feature: Telnet Outbound	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1172497

Defect ID: DEFECT000458826	Technical Severity: Medium
Summary: Log message is not generated when OSPF LSA size exceeds the MTU size of the OSPF interface.	
Symptom: OSPFv3 LS Update with zero LSA, so the OSPF session flapped.	
Feature: OSPFv3	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1171792

Defect ID: DEFECT000458891	Technical Severity: Medium
Summary: The command 'acl-duplication-check' restricts configuring 'deny ipv6 any any' statement.	
Symptom: If 'deny ipv6 any any routing-header-type 0' is configured, 'deny ipv6 any any' statement cannot be configured.	
Feature: ACL - XMR/MLX	Function: IPv6 ACL
Reported In Release: NI 05.4.00	Service Request ID: 1172392

Defect ID: DEFECT000459019	Technical Severity: High
Summary: Specific port on a BR-MLX-100Gx2-X stopped forwarding traffic.	
Symptom: This issue can only happen on the BR-MLX-100Gx2-X in rare circumstances caused by a specific data pattern.	
Feature: IPv4 Forwarding - XMR/MLX	Function: Hardware Forward
Reported In Release: NI 05.4.00	Service Request ID: 1172831

Defect ID: DEFECT000459272	Technical Severity: Medium
Summary: Issuing a LAG deploy after a PCMCIA copy command can cause the standby management modules to unexpectedly reload. If a switchover occurs after the PCMCIA copy, but before the LAG deploy, the active MP may reload.	
Symptom: An active management module unexpectedly reloads only after the following conditions are met: 1) Copying configuration from PCMCIA to running configuration. 2) Management module switchover. 3) LAG deploy. There is no service impact when a standby management module reloads. However, if the active management module reloads, a switchover will occur.	
Feature: Sflow - XMR/MLX	Function: General
Reported In Release: NI 05.2.00	Service Request ID: 1174886

Defect ID: DEFECT000459558	Technical Severity: Medium
Summary: MAC address of a neighbor device is learned on the monitor port when the "output or both" direction is configured.	
Symptom: When a port is configured as the monitor port for an "output or both" direction, the mac-address of a neighbor device connected to another port is learned on the monitor port:	
Feature: CES Mirroring	Function: Port Based
Reported In Release: NI 05.2.00	Service Request ID: 1172690

Defect ID: DEFECT000459817	Technical Severity: Medium
Summary: An interface unexpectedly reloaded due to TM Reset with Offset 0 and value of 0004.	
Symptom: The module will be impacted for 1-2 minutes while it reloads.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.3.00	Service Request ID: 1171573

Defect ID: DEFECT000460162	Technical Severity: High
Summary: 2x100G module throughput is not 100% on an MLX chassis.	
Symptom: When 100G traffic is sent through a 2x100G module, the OutUtilization is ~63G in Normal mode and ~73% in Turbo mode.	
Feature: TM/SFM	Function: Performance (Throughput Latency)
Reported In Release: NI 05.4.00	Service Request ID: 1153825

Defect ID: DEFECT000460394	Technical Severity: Medium
Summary: A CES/CER may unexpectedly reload after issuing a 'show ip' command if the following is configured: 'no ip source-route'; 'no ip icmp mpls-response' and 'no ip forward-protocol udp'.	
Symptom: The CES/CER will take a couple minutes to reload and traffic may be impacted if there is no alternate route.	
Feature: CES IPv4 Forwarding	Function: Routing
Reported In Release: NI 05.4.00	Service Request ID: 1184164

Defect ID: DEFECT000460551	Technical Severity: Medium
Summary: In Software version NI 5.5.00, the command "ipv6 nd global-suppress-ra" is not recognized as a valid command.	
Symptom: After upgrading to 5.5.00 the command "ipv6 nd global-suppress-ra" is no longer configured.	
Feature: IPV6	Function: Neighbor Discovery
Probability: High	
Reported In Release: NI 05.5.00	Service Request ID: 1183445

Defect ID: DEFECT000461211	Technical Severity: High
Summary: TM Fabric Bandwidth feature may have a corrupt message when powering up the link, causing a slot reset.	
Symptom: The system may reload the line card, interrupting traffic.	
Feature: TM/SFM	Function: TM Driver
Reported In Release: NI 05.4.00	Service Request ID: 1168132

Defect ID: DEFECT000461391	Technical Severity: Medium
Summary: Large SCP file transfer followed by any configuration change executed through the CLI causes the standby management module to reset.	
Symptom: Standby reset when large SCP transfer is initiated and at the same time the management port is flapped.	
Feature: Secure Copy	Function: PROTOCOL
Reported In Release: NI 05.2.00	Service Request ID: 1152758

Defect ID: DEFECT000461406	Technical Severity: High
Summary: Greater than Max Age OSPF LSA entries may be seen in a non-default VRF OSPF database.	
Symptom: Stale LSA entries in the OSPF VRF database may cause routes to be missing or LSAs to be unacknowledged, and can potentially cause OSPF session resets.	
Workaround: Configure OSPF instance in default VRF. No further configuration is needed. For example: router ospf area 0	
Feature: OSPF	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.1.00	Service Request ID: 1165356

Defect ID: DEFECT000461813	Technical Severity: Medium
Summary: Available memory declining on 5.4.00b or 5.4.00c on MLX, CES and CER.	
Symptom: Network monitoring tool identified to be causing the memory leak.	
Feature: Chassis/Hw Management	Function: Management Interface
Reported In Release: NI 05.4.00	Service Request ID: 1172071

Defect ID: DEFECT000461822	Technical Severity: High
Summary: In rare condition, when a 100G link is enabled between 2 MLXe-32s, packet drops may occur.	
Symptom: Packet loss is seen.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1187524

Defect ID: DEFECT000462062	Technical Severity: Medium
Summary: 100G ER4 CFP optics is not displaying properly in "sh media".	
Feature: MAC/Phy	Function: Optics Management
Reported In Release: NI 05.5.00	Service Request ID: 1209879,1209879

Defect ID: DEFECT000462097	Technical Severity: Medium
Summary: The device is unable to resolve a DNS name.	
Symptom: Sample output: telnet: abc.com Type Control-c to abort Sending DNS Query to a.b.c.d Ping Failed DNS: Errno(8) DNS query timed out...failed to resolve	
Feature: DNS	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1187621,1202936

Defect ID: DEFECT000462105	Technical Severity: Medium
Summary: After replacing a 4x10G module with an 8x10G, a LAG port in the 8x10G module does not function as expected.	
Symptom: The LAG port in the 8x10G module does not send out known unicast packets.	
Feature: LAG - XMR/MLX	Function: Static
Reported In Release: NI 05.2.00	Service Request ID: 1187833

Defect ID: DEFECT000462367	Technical Severity: Medium
Summary: BGP Graceful Restart Speaker incorrectly generates TCP RST when it reloads itself.	
Symptom: When BGP Graceful Restart Speaker reloads, it generates a TCP RST to terminate the existing BGP session. The BGP Receiving Speaker then treats the routes learned via the session as Graceful routes; so these routes remain, even while the Graceful Restart Speaker is reloaded.	
Feature: BGP	Function: Graceful Restart
Reported In Release: NI 05.4.00	Service Request ID: 1187016

Defect ID: DEFECT000462494	Technical Severity: Medium
Summary: Device is not trying to resolve DNS name.	
Symptom: The sample output below indicates the device is not trying to resolve DNS; rather its response is as though it were working with an invalid IPV6 address. MLX#ping ipv6 abc Ping to IPV6 unspecified addresss not supported!	
Feature: IPV6	Function: ICMP
Reported In Release: NI 05.3.00	Service Request ID: 1188978

Defect ID: DEFECT000463069	Technical Severity: Medium
Summary: Priority force set on ingress port for CFM packets has an unexpected result.	
Symptom: CFM packet replies are missing the VLAN ID and the priority is changed.	
Feature: 802.lag over L2 VLANs	Function: INTEROPERABILITY
Reported In Release: NI 05.2.00	Service Request ID: 1149189

Defect ID: DEFECT000463219	Technical Severity: High
Summary: When 4 power supplies are powered-off on a 32-slot chassis, a fifth power supply fails.	
Symptom: When the fifth power supply fails, two line cards power off.	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1171527

Defect ID: DEFECT000463724	Technical Severity: High
Summary: In a rare condition, low priority traffic may be dropped in the presence of bursty high priority traffic at the ingress line cards (new generation 2x100, 4x40 and 24x10) due to aging.	
Symptom: Low priority traffic was getting dropped in spite of enough bandwidth on the egress port.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1187524

Defect ID: DEFECT000464152	Technical Severity: High
Summary: An unexpected 100GE Module TM Reset Recovery may be performed after an LP Power Cycle.	
Symptom: Additional TM reset causing longer interruption to traffic. Failure of TM to initialize correctly.	
Feature: TM/SFM	Function: TM Driver
Reported In Release: NI 05.4.00	Service Request ID: 1168132

Defect ID: DEFECT000464308	Technical Severity: Medium
Summary: Interface module memory depletes to less than 5% over a period of 6 to 8 months after an LP reboot.	
Symptom: A script is modifying the ACL two to three times every minute, but other devices running the same script do not experience the memory depletion.	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.2.00	Service Request ID: 1171022

Defect ID: DEFECT000464826	Technical Severity: High
Summary: Default route is not originated in to BGP	
Symptom: Default route is missing which can interrupt traffic.	
Workaround: This can be fixed by clearing the OSPF session at ao-e1-pe02 towards the Cisco router which triggers the default route to briefly disappear and then come back into the routing table.	
Feature: BGP	Function: Redistribution
Reported In Release: NI 05.4.00	Service Request ID: 1188142,1190574 / 11

Defect ID: DEFECT000464882	Technical Severity: Medium
Summary: Broadcast packets are looped when LAG ports are on different LPs.	
Symptom: A LAG port that is a VPLS endpoint advertises the MAC learned on another member port.	
Feature: VPLS - XMR/MLX	Function: Forwarding - Single Tunnel
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1193804

Defect ID: DEFECT000464893	Technical Severity: Medium
Summary: After a reload in certain configurations, the L4 ITC Message queue is filled by an aggressive refresh timer.	
Symptom: After reload or mass LP power-cycle, in certain configurations and hardware mixes, the IPv4 and IPv6 rule CAM may not get programmed for modules with PBR applied.	
Workaround: Power cycle each LP individually, waiting for each to come up individually.	
Feature: PBR - XMR/MLX	Function: PBR to VLAN Flooding
Reported In Release: NI 05.4.00	Service Request ID: 1169233

Defect ID: DEFECT000465683	Technical Severity: High
Summary: Link-Keepalive may incorrectly disable the ports on slot 32 of an MLXe-32 chassis.	
Symptom: Ports are disabled by Link-Keepalive, interrupting traffic.	
Feature: UDLD	Function: PROTOCOL
Reported In Release: NI 05.4.00	Service Request ID: 1194842

Defect ID: DEFECT000466113	Technical Severity: High
Summary: After Reload with certain HW and Software configurations, FIDs may not be programmed correctly on some modules.	
Symptom: In certain HW and SW configurations, FIDs may appear as having no ports assigned in some modules, and will not forward traffic.	
Workaround: Power cycle the affected interface modules one at a time.	
Feature: L2 Forwarding - XMR/MLX	Function: Forwarding
Reported In Release: NI 05.4.00	Service Request ID: 1169233

Defect ID: DEFECT000466486	Technical Severity: High
Summary: When forwarding jumbo packets or a sustained high utilization through a 100G module, corruption may occur due to some packet data that is missing.	
Symptom: Packet loss may occur and the TCP checksum will fail, requiring retransmission.	
Feature: FPGA	Function: XPP-8x10
Reported In Release: NI 05.4.00	Service Request ID: 1122271

Defect ID: DEFECT000466583	Technical Severity: High
Summary: An MBGP session over IPv6 neighbor resets due to an update containing MP_REACH_NLRI and no IPv4 update with a next_hop attribute at the end.	
Symptom: The BGP session will go down.	
Feature: BGP	Function: Multicast-BGP
Reported In Release: NI 05.2.00	Service Request ID: 1198324

Defect ID: DEFECT000467383	Technical Severity: Medium
Summary: Console displaying error message every 5-10 minutes.	
Symptom: With SNMP polling enabled for 10-minute intervals, "ERROR:mplp_get_lp_data_request:Session65524: requested slot mask 00000001 00000000 is invalid" is displayed on the console every 5 - 10 minutes.	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1198189,1220700

Defect ID: DEFECT000467729	Technical Severity: Medium
Summary: No warning message is displayed when configured beyond the limitation of 512 VLL instances for CES.	
Symptom: CES currently allows creation of VLL instances beyond the limitation of 512 for both local and remote. No warning or error message is displayed.	
Feature: 802.1ag over VLL	Function: SCALABILITY
Reported In Release: NI 05.4.00	Service Request ID: 1186343

Defect ID: DEFECT000468739	Technical Severity: Critical
Summary: After 24x10G module insertion the last 8 ports (17-24) cannot forward traffic correctly	
Symptom: Ports 17 to 24 cannot forward traffic correctly.	
Feature: System - XMR/MLX	Function: TM
Reported In Release: NI 05.2.00	Service Request ID: 1187406

Defect ID: DEFECT000468956	Technical Severity: Medium
Summary: CER may experience an unexpected reload in SSH task.	
Symptom: The system will take 1-2 minutes to reload.	
Feature: SSHv2	Function: PROTOCOL
Reported In Release: NI 05.3.00	Service Request ID: 1206714

Defect ID: DEFECT000469125	Technical Severity: Medium
Summary: Additional debug code added for traffic forwarding issue.	
Symptom: Connectivity issue seen.	
Feature: IPv4 Forwarding - XMR/MLX	Function: ARP
Reported In Release: NI 05.4.00	Service Request ID: 1207062

Defect ID: DEFECT000469135	Technical Severity: Medium
Summary: LP auto-upgrade does not work for slot 32.	
Symptom: Inserted LP module into slot 32, after module came up FPGA code had not been updated to the correct version.	
Workaround: Insert module into another slot to upgrade images then move to slot 32 or boot into interactive mode and upgrade images manually.	
Feature: Infrastructure Utilities	Function: Image Copy / Download
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1205089

Defect ID: DEFECT000469240	Technical Severity: Medium
Summary: SNMP v3 does not accept AES encryption if AES password string starts with '00'.	
Symptom: When using AES password string which starts with '00' we see that the command gets executed without any error but it does not show up in configuration.	
Feature: SNMP Management	Function: Engine
Reported In Release: NI 05.3.00	Service Request ID: 1206017

Defect ID: DEFECT000469609	Technical Severity: Medium
Summary: In MCT+VPLS, Egress NP replicates broadcast / Multicast incorrectly.	
Symptom: In MCT+VPLS, Egress NP replicates broadcast / Multicast incorrectly after LP is powered off/on or reseated.	
Feature: MCT-VPLS	Function: Hardware Forwarding
Reported In Release: NI 05.4.00	Service Request ID: 1208602

Defect ID: DEFECT000469765	Technical Severity: High
Summary: Memory leak observed after upgrading to 5400c code.	
Symptom: Memory low on one of the CER switches -- "sh tech" does not show the running config .	
Feature: System - XMR/MLX	Function: PERFORMANCE
Reported In Release: NI 05.4.00	Service Request ID: 1209008

Defect ID: DEFECT000469866	Technical Severity: High
Summary: Inter VRF routing is not working for a loopback address.	
Symptom: Inter VRF routing is not working for a loopback address, so can't reach to a loopback address in another vrf.	
Feature: IPv4 Forwarding - XMR/MLX	Function: VRF-lite
Reported In Release: NI 05.5.00	Service Request ID: 1208965

Defect ID: DEFECT000469899	Technical Severity: Medium
Summary: Power supply unit showing less watts compared to actual value in show chassis output	
Symptom: After upgrade from 5200fc to 5200fd the PSU3 AC value changed from 3000W to 2100W	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1209700

Defect ID: DEFECT000470361	Technical Severity: High
Summary: Removal of I2C retry debug messages	
Symptom: Multiple i2c set/clear messages reported in the logs.	
Feature: System - XMR/MLX	Function: POWER SUPPLY
Reported In Release: NI 05.2.00	Service Request ID: 1209698

Defect ID: DEFECT000470570	Technical Severity: Critical
Summary: After modifying the primary LAG port very quickly on MPLS interface, the changes are not getting reflected in RSVP interface which causes MPLS RESV message to drop.	
Symptom: Traffic loss across LSPs reported by monitoring system.	
Feature: MPLS Forwarding - XMR/MLX	Function: Transit LSR
Reported In Release: NI 05.2.00	Service Request ID: 1211401

Defect ID: DEFECT000471321	Technical Severity: High
Summary: After upgrading to 5400c VRRP-e state is master on both the switches for even vlan's in a particular setup.	
Symptom: Prior to upgrading to 5400c code MLX1 is master for all vlan's and MLX2 is backup for all vlans. After upgrade, MLX1 is master for all the vlans and on MLX2 it is showing master for all even vlans and Backup for all odd vlans. So traffic for even vlan's gets black holed.	
Feature: VRRP-E - XMR/MLX	Function: Forwarding
Probability: High	
Reported In Release: NI 05.4.00	Service Request ID: 1209631

Defect ID: DEFECT000471645	Technical Severity: High
Summary: "client-interface delay" command only takes effect on primary LAG port	
Symptom: If the CCEP is an 802.1ad LAG, client-interface delay only takes effect on the primary port of the LAG. On non-primary port(s) the links comes up immediately.	
Feature: MCT	Function: LACP
Reported In Release: NI 05.4.00	Service Request ID: 1212893

Defect ID: DEFECT000471703	Technical Severity: Medium
Summary: Erroneous snAgentBrdIndex is set in snTrapModuleRemoved.	
Symptom: When removing Standby Management Module, erroneous snAgentBrdIndex is set over snTrapModuleRemoved. Erroneous snAgentBrdIndex is set only when 1st removing Standby Management Module after chassis comes up. The erroneous snAgentBrdIndex is seen only the 1st time removing Standby Management module: after that the correct snAgentBrdIndex.34 is set.	
Feature: SNMP Management	Function: Platform Mib
Reported In Release: NI 05.4.00	Service Request ID: 1211105

Defect ID: DEFECT000472111	Technical Severity: Critical
Summary: A packet is routed via VE over VPLS that has a route lookup hit of the destination network. When the hardware sends it to the CPU, it may trigger a reload of the ingress linecard.	
Symptom: There will be service impact to the ports on this interface module for about 1 minute while the module reloads.	
Feature: Linecard / XPP	Function: PBIF TXA / RXA
Reported In Release: NI 05.4.00	Service Request ID: 1217702