BROCADE

Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family

Release Notes v2.0

September 28, 2010

Document History

Document Title	Summary of Changes	Publication Date
Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family Release Notes v.1.0	Initial release	September 20, 2010
Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family Release Notes v.2.0	The following corrections have been made to these release notes: 2 defects added to the closed section Image names corrected Copy secondary command re-inserted	September 28, 2010

Contents

Supported devices for Multi-Service IronWare R05.1.00

This software release applies to the following Brocade products:

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

Supported features for Brocade MLXe and NetIron family devices

The following tables describe all of the features supported on the Brocade MLXe, and NetIron family devices. Features or options not listed in these tables, and not documented in the *NetIron Configuration Guide* are not supported. For a list of unsupported features, see the "Unsupported Features" section following this section.

Table 1   List of supported features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
System Level Features								
Cisco Discovery Protocol (CDP)	Allows you to configure a device to intercept and display the contents of CDP packets. This feature is useful for learning device and interface information for Cisco devices in the network.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Foundry Discovery Protocol (FDP)	Enables the devices to advertise themselves to other devices on the network.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Denial of Service (DoS) Protection	Protection from SYN attacks Protection from Smurf attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLI Logging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management Options	Serial, Telnet and SSH access to industry-standard Command Line Interface (CLI) SSHv2 TFTP and SCP SNMP versions 1, 2, and 3 IronView Network Manager.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management Options	Web GUI	Yes	Yes	No	No	No	No	No

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
High Availability	Hitless Software Upgrade Hitless Layer 2 Failover Hitless Layer 3 Failover (BGP and OSPF) IPv4 Multicast (IGMP, PIM-DM, PIM-SM, PIM-SSM)	Yes	Yes	No	No	No	No	No
IP Security	Dynamic ARP Inspection (DAI) DHCP Snooping DHCP with Option 82 Insertion	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	IP Source Guard	Yes	Yes	No	No	No	No	No
Security	AAA Login Authentication using RADIUS, TACACS, TACACS+, local account, enable and line passwords AAA Enable Authentication using RADIUS, TACACS, TACACS+, local account, enable and line passwords AAA Command Authorization using RADIUS, TACACS+ AAA Command Accounting using RADIUS, TACACS+ AAA EXEC Accounting using RADIUS, TACACS+ Local passwords Secure Shell (SSH) version 2 Secure Copy (SCP) User accounts AES for SNMPv3 AES for SSHv2 Note: Telnet, SSH and SNMP servers are disabled by default, and can be enabled selectively.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Logging	Multiple SysLogD server logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
sFlow	sFlow version 5 ACL-based sFlow	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Jumbo Packets	Jumbo Packet Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family Release Notes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Uni-Directional Link Detection (UDLD)	Monitors a link between two devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UDLD on tagged ports	Allows ports to send out UDLD control packets that are tagged with a specific VLAN ID as tagged UDLD control packets.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced User Password Combination		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ACL Accounting	Global statistics for inbound and outbound packets denied by ACLs	Yes	Yes	No	No	No	No	No
	Filter-level (per clause) statistics for inbound and outbound packets denied by ACLs	No	No	Yes	Yes	Yes	Yes	Yes
Layer 2 Features								
IEEE 802.1d	Spanning Tree Protocol (STP) within the default ESI (Ethernet Service Instance) Single Spanning Tree Protocol (SSTP) within the default ESI (Ethernet Service Instance)	No	No	No	Yes	No	No	Yes
IEEE 802.1d	Spanning Tree Protocol (STP) Single Spanning Tree Protocol (SSTP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.1p	Class of service for traffic prioritization	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.1q	Refer to VLANs, below	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP) within the default ESI (Ethernet Service Instance). and Single Spanning Tree Protocol (SSTP) within the default ESI (Ethernet Service Instance).	No	No	No	Yes	No	No	Yes
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP) Single Spanning Tree Protocol (SSTP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.1s	Multiple Spanning Tree Protocol within the default ESI (Ethernet Service Instance).	No	No	No	Yes	No	No	Yes
IEEE 802.1s	Multiple Spanning Tree Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.1x	Port Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.3ad	Link Aggregation Control Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2 ACL	Filtering based on MAC layer-2 parameters.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CPU Protection	Enhances the efficiency of the CPU on an Interface module and protects it from an excessive amount of network traffic.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MAC Port Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast	IGMP v1, v2, v3 snooping PIM-SM snooping (IPv4 only) Prune Wait Timer for PIM DM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Concurrent multicast routing and snooping for IPv4	Yes	Yes	No	No	No	No	No
Foundry MRP	Foundry Metro Ring Protocol (MRP) Phase 1 and Phase 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
PVST or PVST+	Per-VLAN Spanning Tree (PVST) within the default ESI (Ethernet Service Instance).	No	No	Yes	No	No	Yes	Yes
PVST or PVST+	Per-VLAN Spanning Tree (PVST)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SuperSpan	A Brocade STP enhancement that allows Service Providers (SPs) to use STP in both SP networks and customer networks.	Yes	Yes	No	No	No	No	No
Topology Groups	A named set of VLANs that share a Layer 2 topology. You can use topology groups with the following Layer 2 protocols: STP MRP VSRP IEEE 802.1W	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Link Aggregate Groups (LAGs)	Allows you to manually configure multiple high-speed load-sharing links between two switches or routers.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Uplink-Switch	Isolated Private VLANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VLANs	IEEE 802.1q tagging Port-based VLANS Dual-Mode VLAN Ports VLAN Transparent Hardware Flooding	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VLANs	Super Aggregated VLANs (SAV) VLAN Translation Protocol-Based VLANs	Yes	Yes	No	No	No	No	No
VSRP	Virtual Switch Redundancy Protocol (VSRP) VSRP-fast start	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VSRP - MRP Signaling		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Advanced Layer 2 Features								
Ethernet Service Instance (ESI)	RSTP and STP for C-VLANs, S-VLANs and B-VLANs when using the ESI framework	Yes	No	No	Yes	No	No	Yes
	MRP and MRP-II for C-VLANs, S-VLANs and B-VLANs when using the ESI framework							
	Topology groups within an ESI							
	VLAN groups within an ESI							
	Static LAG (LAG groups) within an ESI							
IEEE 802.1ad	Provider Bridges	No	No	No	Yes	No	No	Yes
IEEE 802.1ag	Connectivity Fault Management (CFM) for C-VLANs, B-VLANs, and S-VLANs within an ESI Connectivity Fault Management within the default ESI	No	No	No	Yes	No	No	Yes
	Connectivity Fault Management (CFM) for C-VLANs only	Yes	Yes	No	Yes	No	No	Yes
IEEE 802.1ah	Provider Backbone Bridges	No	No	No	Yes	No	No	Yes
Layer 2 Protocol Forwarding	This feature only forwards STP and RSTP customer side packets.	No	No	No	Yes	No	No	Yes
Layer 3 Features								
IPv4 ACLs	Standard and Extended Inbound and Outbound ACL logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
BGP	BGP routes BGP peers BGP dampening BGP Confederations BGP Route Reflectors Multi-hop E-BGP Community filters Restart helper mode Multipath load sharing MD5 authentication BGP4 MIB and notification per RFC 4273 Multi-protocol BGP Extended Communities Route Refresh Co-operative BGP Route Filtering Graceful Restart Helper Change BGP default of BGP MED for route cost to IGP cost	Yes	Yes	No	No	Yes	Yes	Yes
	Graceful Restart	Yes	Yes	No	No	No	No	No
FDR	Foundry Direct Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Forwarding	IPv4 Routing IPv6 Routing Secondary Addresses	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Static Entries	Routes ARP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IS-IS	Routes Adjacencies LSPs MD5 Authentication 3-Way Handshake for Pt-to-Pt Adjacencies BFD for IS-IS IS-IS Black Hole Avoidance PSPF Optimizations	Yes	Yes	No	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
IS-IS (continued)	Traffic Engineering Extensions	Yes	Yes	No	Yes	No	No	Yes
IPv4 Multicast Routing	IGMP v1, v2, v3 PIM-DM PIM-SM PIM-SSM MSDP Anycast RP Prune Wait Timer for PIM DM	Yes	Yes	No	Yes	Yes	Yes	Yes
OSPF	OSPF routes OSPF adjacencies – Dynamic OFPF LSAs OSPF filtering of advertised routes MD5 authentication Restart helper mode BFD for OSPF OSPF Administrative Distance Control Using Route Maps OSPF Dynamic Metric Calculation for Trunks/VE Interfaces OSPF VRF-Lite for CE routers	Yes	Yes	No	Yes	Yes	Yes	Yes
	Graceful Restart Traffic Engineering (TE) Extensions	Yes	Yes	No	Yes	No	No	Yes
	Graceful Restart Helper	Yes	Yes	No	No	Yes	Yes	Yes
Policy-Based Routing (PBR)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-VRF	Multi-VRF for IPv4 Unicast (OSPF and Static)	Yes	Yes	No	Yes	Yes	Yes	Yes
	Multi-VRF for IPv4 Unicast (BGP)	Yes	Yes	No	No	Yes	Yes	Yes
RIP Versions 1 and 2	RIP routes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
VRRP and VRRPE	Virtual Router Redundancy Protocol (VRRP) and VRRP Extended (VRRPE)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

QoS Features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Traffic Policing	The following rate limiting types are available on inbound and outbound ports: Port-based Port-and-ACL-based (Both L2 and L3 ACLs) Hardware-based rate limiting of CPU-copied traffic	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Port-and-priority-based VLAN-based VLAN-group-based (outbound only) VLAN and priority based VLAN-group and priority based (outbound only)	Yes	Yes	No	No	No	No	No
Traffic Scheduling	The following scheduling schemes are supported: Strict Priority (SP) Scheduling	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Weighted Fair Queuing (WFQ) scheduling Mixed SP and WFQ scheduling	Yes	Yes	No	No	No	No	No
	Weighted Round Robin (WRR) Scheduling Mixed SP and WRR Scheduling	Yes	No	Yes	Yes	Yes	Yes	Yes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
VPN Features								
Topology Groups	Named set of VLANs and VPLS endpoints that share a Layer 2 topology. Use topology groups with these Layer 2 protocols: • STP • Brocade MRP • VSRP • IEEE 802.1w	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 VPN	VPLS • Local VPLS (without MPLS) VLL • Local VLL • Single Tag	Yes	Yes	No	Yes	No	No	Yes
	VPLS • Multicast Snooping for VPLS • IGMP and PIM Proxy for VPLS • Disabling of VPLS Local Switching • BGP Auto-Discovery • Double Tag • VPLS cpu protection	Yes	Yes	No	No	No	No	No
Layer 3 VPN (Requires ME_PREM plus L3_PREM licenses)	BGP/MPLS VPNs (RFC 2547bis) • OSPF Sham Link Support • Support for RFC 4382: MPLS-L3VPN Standard MIB • Multi-VRF • Per-VRID virtual MAC address assignment • Per-VRF VRRP-E • Static Routes Across VRFs	Yes	Yes	No	Yes*	Yes*	No	Yes
IPv6 Features								
IPv6 ACLs	Extended ACLs	Yes	Yes	No	Yes	Yes	Yes	Yes

Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family Release Notes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
IPv6 Routing Protocols	RIPng IS-IS for IPv6 OSPFv3 IPsec Authentication	Yes	Yes	No	Yes	Yes	Yes	Yes
	BGP4+	Yes	Yes	No	No	Yes	Yes	Yes
IPv6 Multicast Routing	MLD v1, v2 PIM-SSM PIM-SM Anycast RP	Yes	Yes	No	Yes	Yes	Yes	Yes
MPLS Features								
MPLS	LDP RSVP-TE OSPF-TE ISIS-TE LSR Support OAM - LSP ping and LSR Traceroute (only on Ingress and Egress routers) VPLS and VLL Hot-standby LSPs VPLS and VLL support LAG endpoints from VPLS and VLL MPLS over LAG Fast Reroute Detour Support CSPF Adaptive LSPs	Yes	Yes	No	Yes	No	No	Yes
	BFD for RSVP-TE Fast Reroute Bypass Support LSP Accounting OAM - LSP ping and Traceroute	Yes	Yes	No	No	No	No	No

Unsupported features

Unsupported features in Brocade MLXe, NetIron MLX, and NetIron XMR devices

The following features are not supported in software R05.1.00 on the Brocade MLXe, NetIron MLX, and NetIron XMR series routers:

- IPv6 - The following IPv6 features are not supported in this release:

  AAA using IPv6
  Packet filtering based on the IPv6 flow label
  IPv6 anycast address

- NAT

- RARP

- Private VLANs

- GVRP

- Static LSPs

- Switch LAGs

Unsupported features NetIron CES series and NetIron CER devices

The following features are not supported in software R05.1.00 on NetIron CES series and NetIron CER series devices:

- NAT

- GVRP

- Static LSPs

- SuperSpan - Supports Layer 2 protocol forwarding

- Private VLANs - Supports private VLANs with S-Vlans and uplink-switch with regular VLANs

- Super Aggregated VLANs (SAV). Supports Provider Bridging as per IEEE 802.1ad, which supersedes SAV

- Protocol-based VLANs

- Web Based GUI

- Hot swapping of 10-Gig modules

Not applicable features

The following features are not applicable in software R05.1.00 on NetIron CES and NetIron CER devices:

- Hitless Management Failover

- Hitless Upgrade

- Packet Over SONET (POS)

Summary of enhancements for Multi-Service IronWare R05.1.00

The following sections list the enhancements in the most recent major releases. Because the NetIron XMR and NetIron MLX code is now merged with the NetIron CER and NetIron CES code, enhancements added in R05.1.00 are described as follows:

- "New" indicates that the feature was added to the specified platform in the current release

- "Supported" indicates that the feature was added to the specified platform in an earlier release

- "Not supported" indicates that the feature is not currently supported on the specified platform

System features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Software-based Licensing	Software-based licensing provides increased scalability and rapid deployment of hardware and software features on the supported NetIron XMR and NetIron MLX line cards. See "Software-based Licensing" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Supported	Supported	Supported	Supported	Supported
IS-IS Non-Stop Routing (NSR)	IS-IS Non-Stop Routing (NSR) enables the IS-IS router to maintain topology and data flow to avoid re-convergence in the network during a processor switchover or hitless-reload event. See "IS-IS Non-Stop Routing" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Management VRF	Management VRF is a special VRF defined for all inbound and outbound access to the device. See "Management Virtual Routing and Forwarding (VRF)" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Limiting Link Negotiation Speed to 100M	Allows you to reduce or limit the port speed when auto- negoiation is configured. See "Auto Negotiation Speed Limit" in the Brocade MLXe and Brocade MLXe and NetIron Family Configuration Guide.	Not Supported	Not Supported	New	New	New	New	New
Real-Time Monitoring	Allows you to display traffic statistics in real time for a single Ethernet port or for all ports. See "Monitoring Ethernet port statistics in real time" in Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New
Automatic Switch Fabric Module Shutdown	Automatically shuts down an SFM when errors are detected. See "Powering a switch fabric module off automatically on failure" in Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Protocol features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
OSPF VRF-Lite for CE Routers	Allows configuration of VRF-lite functionality on CE router. Refer to "OSPF VRF-Lite for customer-edge routers" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	New	New	New
VRRP Virtual MAC address per VRID	Allows manual assignment of a virtual MAC address per VRID. Refer to "Configuring unique virtual MAC addresses per VRID" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
BGP - use IGP cost	Overrides default BGP MED to use IGP cost when adding routes to the RTM. See "Changing the default metric used for route cost" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	New	New	New
Add name for static route	Assign a name to a static IP route as a description of the route to easily reference or identify the associated static route. See "Naming a static IP route" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New
Dual tag types	Dual tag types within an ESI are now supported on the NetIron CES and NetIron CER. See "Tag-type configuration" in the Brocade MLXe and Brocade MLXe and NetIron Family Configuration Guide	Not Supported	Not Supported	Not Supported	New	Not Supported	Not Supported	New
Supress receipt and announcement of BGP prefixes with hugh AS-paths	Use the maxas-limit in command to configure a router running BGP4 to discard routes that exceed a specified AS path limit. Can be configured globally, for peer groups, and for BGP neighbors. See "Specifying a maximum AS path length" in the Brocade MLXe and Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	New	New	New
VRRP-E for IPv6	Multi-Service IronWare now supports VRRP-E for IPv6, a proprietary version of VRRP that overcomes limitations in the standard protocol. See "Configuring VRRP and VRRP-E" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	New	New	New
VRRPv3 for IPv4	This release adds support for VRRPv3 for IPv4. See "Configuring VRRP and VRRP-E" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New
VRRPv3 for IPv6	This release adds support for VRRPv3 IPv6. See "Configuring VRRP and VRRP-E" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
sFlow for MLPS	This release provides sFlow support for MPLS endpoints. See "sFlow support for MPLS" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New	Not Supported	Not Supported	New
Ethernet Ring Protection (ERP)	Integrates an Automatic Protection Switching (APS) protocol and protection switching for Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies. See "Ethernet Ring Protection" in the *Brocade MLXe and NetIron Family Configuration Guide.*	New	New	New	New	New	New	New
TTL Threshold for IPv4 and IPv6Routed Multicast Packets	This feature, defines the minimum TTL value required in a multicast packet for it to be forwarded out of the interface. See "Modifying the TTL threshold" and "Modifying the Hop-Limit threshold" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New	New	New	New
MLDv1, MLDv2 support	In this release, support for MLDv1 and MLDv2 was added to the NetIron CES and NetIron CER. See "Multicast Listener Discovery and source specific multicast protocols" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New	New	New	New
PIM-SM and PIM-SSM support for IPv6	In this release, the NetIron supports IPv6 Protocol Independent Multicast (PIM) Sparse. IPv6 PIM Sparse provides multicasting that is especially suitable for widely distributed multicast environments. See "IPv6 PIM Sparse" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New	New	New	New

Multi-Service IronWare Software R05.1.00 for Brocade NetIron Family Release Notes

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
IPv6 Multicast routing support	This release supports IPv6 Multicast routing on the NetIron CES and NetIron CER. See "Configuring IPv6 Multicast Features" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New	New	New	New
LDP tImers per interface	This feature allows you to set separate LDP Hello Intervals and LDP Hello Hold Times for specified interfaces. See "Setting the LDP Hello Interval and Hold Timeout values" and "Displaying information about specified LDP-enabled interface" in the *Brocade MLXe and NetIron Family Configuration Guide*.	Supported	Supported	Not Supported	New	Not Supported	Not Supported	New
IPv6 anycast RP for PIM-SM	This release supports PIM Anycast RP for IPv6 multicast domains. PIM Anycast RP is a method of providing load balancing and fast convergence to PIM RPs in an IPv6 multicast domain. See "PIM Anycast RP" in the *Brocade MLXe and NetIron Family Configuration Guide*.	Supported	Supported	Not Supported	New	New	New	New
Multicast boundary for IPv6	Beginning with this release, Multicast boundaries can be configured for IPv6. The Multicast Boundary feature provides the ability to selectively allow or disallow multicast flows to configured interfaces. See "Configuring multicast boundaries" in the *Brocade MLXe and NetIron Family Configuration Guide*.	Supported	Supported	Not Supported	New	New	New	New

MPLS features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Layer 3 VPN (Requires both ME_PREM and L3_PREM License on the NetIron CES)	In this release, Layer 3 VPNs are supported on the NetIron CES and NetIron CER. See "Configuring BGP or MPLS VPNs" in the Brocade MLXe and NetIron Family Configuration Guide.	Supported	Supported	Not Supported	New (Requires both ME_PREM and L3_PREM License on the NetIron CES)	New (Requires both ME_PREM and L3_PREM License on the NetIron CES)	Not Supported	New
LDP over RSVP (for transit LSR only)	LDP over RSVP (for transit LSR only) enables LDP traffic to tunnel across RSVP tunnels. The RSVP tunnel is the transit of the LDP tunnel. See "LDP over RSVP (for transit LSR only)" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	Not Supported	Not Supported	New
LDP ECMP for transit LSR	LDP Equal-Cost Multi-Path (ECMP) for transit LSR provides ECMP support for transit routers on an LDP LSP. See "LDP ECMP for transit LSR" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Display changes for MPLS show commands for long LSP and Path names	The following MPLS show commands are enhanced to display the full LSP name in a single line. Previously, a long LSP name (greater than 12 characters) was text-wrapped in multiple lines. • show mpls lsp wide • show mpls path wide • show mpls bypass-lsp wide • show mpls rsvp-session wide • show mpls rsvp-session wide backup See "Displaying signalled LSP status information", "Displaying path information", "Displaying bypass LSPs", and "Displaying RSVP session information" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	New	Not Supported	Not Supported	New

Layer 2 features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
64- port LAG	Change the number of LAGs and member ports using the system-max trunk-num num command. Valid values are 32, 64, 128, and 256. By default, the router is configured to support 128 LAGs with each containing 16 member ports.See "LAG formation rules" in the Brocade MLXe and Brocade MLXe and NetIron Family Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Multi-Chassis Trunk (MCT)	A Multi-Chassis Trunk (MCT) initiates at a single MCT-unaware server or switch and terminates at two MCT-aware switches. See "Multi-Chassis Trunking (MCT)" in the Brocade MLXe and Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New

Management features

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
RFC support on NetIron CES and NetIron CER	RFC 4022 (TCP MIb), RFC 4113 (UDP MIb)RFC 4382 (L3VPN MIB) are now supported on NetIron CES and NetIron CER.	Supported	Supported	New	New	New	New	New
	RFC 4382 (L3VPN MIB) are now supported on NetIron CES and NetIron CER.	Supported	Supported	Not Supported	New (Requires both ME_PREM and L3_PREM License on the NetIron CES)	New (Requires both ME_PREM and L3_PREM License on the NetIron CES)	Not Supported	New

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
New and updated objects for software licensing	The following objects are new in this release: fdryLicenseSlot indicates which slot and module has been licensed fdryLicensedFeatureInfo indicates which feature is licensed. Also, fdryLicenseHash, one of the objects used to indes the fdryLicenseTable, has been changed to IMPLIED fdryLicenseHash In addition, Software Licensing support for the NetIron XMR, NetIron MLX, and Brocade MLXe has been added to this release.	New	New	New	New	New	New	New
New Switch Fabric Module notification	The snTrapSFMStatusChange notification is generated when there is a change in the operational state of the Switch Fabric Module	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Enhancements in snChassis MIBs for serial and part numbers	The following objects provide information for part and serial numbers: • snChasIdNumber now displays the distributor part number • snChasSerNum now displays the distributor serial number • snChasFactoryPartNumber, a new object, displays the vendor part number • snChasFactorySerialNumber, new object, displays the vendor serial number	New	New	New	New	New	New	New
Rate-limiting counters displayed in the ACL table	Updated MIB object agAclAccntTable and added support for agAclAccntRaclDropCnt, agAclAccntRaclFwdCnt, agAclAccntRaclRemarkCnt, agAclAccntRaclTotalCnt to return the RL stats for L2ACL. See "Displaying accounting information for rate limit usage" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX and Brocade MLXe Series	NetIron CES 2000 Series BASE package	NetIron CES 2000 Series ME_PREM package	NetIron CES 2000 Series L3_Prem package	NetIron CER 2000 Series BASE package	NetIron CER 2000 Series Advanced Services package
Interactive Multi-factor RADIUS Security Support	Interactive log-in supports multi-factor authentication for RADIUS security (e.g., for RSA SecurID). See "Multi-factor RADIUS authentication" in the Brocade MLXe and NetIron Family Configuration Guide.	New	New	New	New	New	New	New
SNMP support for the Brocade MLXe chassis	SNMP support for the Brocade MLXe has been added as follows: The snChasProductType SNMP object has been enhanced to include four new enumeration values for the new chassis models. • The snChasSystemMode object has been added which indicates if the chassis is an XMR, MLX, or MLXe • Registration objects have been added for the MLXe models For the new MLXe devices, sysDescr scalar MIB variable returns the appropriate description for the device. For example: `Brocade Communications Systems, Inc. MLXe (System Mode: XMR), IronWare Version V5.0.0T163 Compiled on Nov 17 2009 at 22:38:57 labeled as V5.0.00` The new objects are discussed in the following chapters of the *IronWare MIB Reference*: • "General chassis" section of the "Physical Properties of a Device" chapter • "Registration" chapter	Not applicable	New	Not applicable	Not applicable	Not applicable	Not applicable '	Not applicable

Software Upgrade Instructions

The following sections describe the steps necessary to upgrade your Multi-Service IronWare software. The following table shows you where to find information specific to your upgrade needs.

Where to find upgrade instructions for your router type and configuration

If you are upgrading:	Go to these sections, (in the order listed):
All Brocade MLXe, NetIron MLX, and NetIron XMR devices: First read "Important software upgrade information for Brocade MLXe, NetIron MLX, and NetIron XMR routers"	

Brocade MLXe routers	
Determine current image versions	"Displaying version information for Brocade MLXe, NetIron MLX, and NetIron XMR routers"
Routers with 10x8G modules	"Interface module upgrade considerations" "Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices"
Routers with a management module running pre-05.0.00 software	"Special upgrade information for Brocade MLXe routers" Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices
Upgrade Interface modules using combined FPGA image	"Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices" "Upgrade interface modules using the combined FPGA image"
Upgrade interface module FPGA images individually	"Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices" "Upgrading individual FPGA images on interface modules"
When you have finished upgrading all images	"Performing a coherency test" "Rebooting the management module"
NetIron MLX and NetIron XMR routers	
Determine current image versions	"Displaying version information for Brocade MLXe, NetIron MLX, and NetIron XMR routers"
Running R05.0.00 software	"Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices"
Running pre- R05.0.00 software	"Legacy upgrade information for Brocade MLXe, NetIron MLX, and NetIron XMR devices"
With 10x8G modules	"Upgrading to R05.1.00 for routers with NI-MLX-10Gx8 modules"
With 10x8G modules, and while installing high speed switch fabric modules	"Upgrading to R05.1.00 while installing high-speed switch fabric modules and NI-MLX-10Gx8 modules"
32-slot switch fabric modules	"Upgrading the SBRIDGE image on switch fabric modules for 32-slot devices"
Upgrade Interface modules using combined FPGA image (R05.0.00c and later only)	"Upgrade interface modules using the combined FPGA image"
Upgrade interface module FPGA images individually	"Upgrading individual FPGA images on interface modules"
When you have finished upgrading all images	"Rebooting the management module" "Performing an image coherency check"
NetIron CER and CES devices:	

Determine installed image versions	"Displaying version information for NetIron CER and NetIron CES devices"
Upgrading from R05.0.00 to R05.1.00	"Upgrading from R0.5.0.00 to R05.1.00 for NetIron CER and NetIron CES devices"
When you have finished upgrading all images	"Rebooting the management module" "Performing an image coherency check"

Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR devices

The following sections describe how to upgrade your Multi-Service IronWare software from R05.0.xx to R05.1.00. If you are upgrading to R05.1.00 from versions prior to R05.0.xx, refer to "Legacy Software Upgrade Information for NetIron MLX and NetIron XMR devices."

Performing a basic upgrade

The following sections describe the steps for a basic upgrade from R05.0.xx to R05.1.00.

Note: If your system fits any of the scenarios described in "Important software upgrade considerations for Brocade MLXe, NetIron MLX, and NetIron XMR routers", you will not be able to perform a basic upgrade. Refer to the table "Where to find upgrade information for your router type and configuration" for special upgrade instructions.

The following table lists the *minimum* required images and image names to upgrade to R05.1.00.

Required images for R05.1.00 upgrade

Required image	Image name
Combined application image for management modules	xm05100.bin
Monitor image for management modules	xmb05100.bin
Monitor image for interface modules	xmlb05100.bin
Boot image for management modules	xmprm05100.bin
Boot image for interface modules	xmlprm05100.bin
Combined FPGA image for interface modules	lpfpga05100.bin

NOTE: The software described in this section applies only to the Brocade MLXe, NetIron MLX, and NetIron XMR series routers. You cannot use this software on other Brocade devices.

Minimum required steps to upgrade from R05.0.xx to R05.1.00

The process for upgrading your software from R05.0.xx to R05.1.00 requires the minimum steps shown in this section.

For non-standard upgrades, and special software upgrade considerations, see "Important information about software upgrade information for Brocade MLXe, NetIron MLX, and NetIron XMR routers."

If you are upgrading to R05.1.00 from versions *prior* to R05.0.xx, refer to "Legacy Software Information."

Step 1 – Determine the software versions currently running on your system. If your system is running image versions that are not listed in the table "Software images for R05.1.00 for Brocade MLXe, NetIron MLX, and

NetIron XMR routers", you will need to upgrade those images as well as the standard required images. Refer to "Additional upgrade steps."

If your system is not running any incompatible image versions, proceed to step 2.

Step 2 – Upgrade the combined application image on all management modules. Refer to "Upgrading the combined application image on management modules."

Step 3 – Upgrade the monitor image for management modules and interface modules. Refer to "Upgrading the monitor image for management modules" and "Upgrading the monitor image for interface modules."

Step 4 – Upgrade the boot images for management modules and interface modules. Refer to "Upgrading the boot image for management modules" and "Upgrading the boot image for interface modules."

Step 5 – Upgrade the combined FPGA image on interface modules. Refer to "Upgrading the combined FPGA image on interface modules.

Step 6 – Perform a coherency check. Refer to "Performing an image coherency check."

Step 7 – Reboot the management module. Refer to "Rebooting the management module."

The following table lists all of the images for R05.1.00.

Software images for R05.1.00

Hardware	Image type	Image name	Compatible version
Management modules	Boot Monitor Application Combined Application MBRIDGE MBRIDGE32	xmprm05100.bin xmb05100.bin xmr05100.bin xm05100.bin mbridge_05100.xsvf mbridge32_05100.xsvf (32-slot routers only)	n/a n/a n/a n/a 32 32
Interface modules	Boot Monitor Application Combined FPGA FPGA (individual)	xmlprm05100.bin xmlb05100.bin xmlp05100.bin lpfpga05100.bin pbifsp2_05100.bin (all Ethernet modules except Mini-RJ)	n/a n/a n/a n/a 3.22
		xppsp2_05100.bin (all Ethernet modules except Mini-RJ)	6.04
		xppoc_05100.bin (POS interface modules only)	6.01
		pbifoc_05100.bin (POS interface modules only)	3.05
		statsoc_05100.bin (POS interface modules only)	2.06
		pbifmrj_05100.bin (NI-MLX-1Gx48T-A modules only)	3.24
		xppmrj_05100.bin (NI-MLX-1Gx48T-A modules only)	6.03
		statsmrj_05100.bin (NI-MLX-1Gx48T-A modules only)	0.08
		pbif8x10_05100.bin (NI-MLX-10Gx8 modules only)	0.28
		xpp8x10_05100.bin (NI-MLX-10Gx8 modules only)	2.14
		xgmacsp2_05100.bin (4x10modules)	0.13
Switch fabric modules	SBRIDGE	sbridge_05100.mcs	6
High speed switch fabric modules	HSBRIDGE	Hsbridge_05100.mcs	16

Important software upgrade considerations for Brocade MLXe, NetIron MLX, and NetIron XMR routers

Read the following information carefully before you begin your software upgrade.

General upgrade considerations

- The combined interface module FPGA image can exceed 32 MB in size, which is greater than the file size limit in older versions of TFTP server applications. Before using TFTP to transfer image files, be sure that you are using an updated TFTP server capable of handling larger file sizes.

- In most cases boot and monitor images do not need to be upgraded, regardless of whether you are using the combined IronWare image, or are copying images to the management module and interface modules individually. Do not upgrade boot or monitor images unless you are explicitly instructed to do so in the upgrade instructions for the version you are using.

- Hitless OS upgrades are only supported for upgrades within the same major software release. Hitless OS upgrades are not supported for upgrades from one major release to another major release. For more information about hitless upgrades, refer to "Hitless OS Upgrades".

Special upgrade information for Brocade MLXe routers

- Brocade MLXe routers require a minimum software release of 5.0.00c.
- In rare circumstances, you may receive management modules that are running R04.0.00b or R04.0.00g. In this instance, follow the instructions below to upgrade the management module and the MLXe router to R05.1.00.
- If you plan to use a management module from an existing NetIron MLX or NetIron XMR router in your Brocade MLXe router, you must first upgrade the management module to R05.0.00c or later, then transfer it to the MLXe chassis.

Installing an R04.0.00b or R04.0.00g management module in a Brocade MLXe router

In some instances, you may want to transfer a management module running R04.0.00b or R04.0.00g software from a NetIron MLX or NetIron XMR chassis to your Brocade MLXe router. If you do not upgrade the management module **before** you install it in the MLXe router, when you boot the router the following message will be displayed:

```
"Error: unknown chassis type value 000000f0, system can't come up!"
```

To correct this, enter **CTRL-Y-M** to go to the OS Mode in the CLI. In the OS mode, copy the R05.1.00 management module application, boot, and monitor images to the management module, and then restart the router. For example:

```
telnet@Router1# rconsole
Remote connection to MP local port established
Press CTRL-X or type exit to disconnect it
Router1(config)#
MP-1 OS>copy tftp flash 1.1.1.1 ?
boot            to boot flash
monitor         to monitor image
primary         to primary image
secondary        to secondary image
String          to a named file
MP-1 OS>copy tftp flash 1.1.1.1 xmr05000.bin primary
MP-1 OS>copy tftp flash 1.1.1.1 xmb05000.bin monitor
MP-1 OS>copy tftp flash 1.1.1.1 xmprm05000.bin boot
```

Upgrading Brocade MLXe management modules running R04.0.00b or R04.0.00g software

In rare instances, a Brocade MLXe router may ship with a management module running R04.0.00b or R04.0.00g software. In this case, you must upgrade the R04.0.00g software to R05.1.00. If you boot a Brocade MLXe router with a management module that is running R04.0.00g software, the router will be recognized as a NetIron XMR router. To correct this, and have the router correctly identified, *before* you upgrade the management module to R05.1.00, you must delete the **primary** and **lp-primary-0** files on the management module, by entering the following commands:

```
MP# delete primary
MP# delete lp-primary-0
```

Note: If the flash memory contains additional files not related to the software upgrade, it is recommended that you also delete these files to free up memory.

You must also delete the **primary** image from flash memory on the interface modules. Establish an rconsole connection to each interface module and enter the **delete primary** command as shown.

```
NetIron# rconsole 2
Remote connection to LP slot 2 established
Press CTRL-X or type exit to disconnect it
LP-2>en
No password has been assigned yet...
LP-2# del primary
```

You are now ready to upgrade your router to R05.1.00. Proceed to "Upgrading from R05.0.xx to R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR routers."

Interface module software upgrade considerations

The following sections contain important upgrade information for interface modules.

Interface module FPGA image upgrade considerations

Note: You must use FPGA images that are specified for Brocade MLXe, NetIron MLX, or NetIron XMR series routers. Use of FPGA images intended for other products will render your chassis inoperable.

The following rules apply when upgrading FPGA images on interface modules:

- FPGA images on interface modules must be compatible with the software version running on the router.

- You can upgrade FPGA images individually, or upgrade all FPGA images using the combined FPGA image.

- When you copy the combined FPGA image from to the management module, the management module selects the FPGA images to be downloaded based on the types of interface modules installed and checks for duplicates before downloading the images.

- The FPGA upgrade utility compares the FPGA image version currently installed to new images being downloaded. If the versions are identical, the download is aborted and a warning message is displayed. You can use the **force-overwrite** option with the FPGA upgrade command to override this feature.

- The bundled FPGA image is more than 32 MB in size. If you are using a TFTP server, be sure that it is capable of handling larger file sizes.

Considerations for NI-MLX-10Gx8 interface modules requiring high-speed switch fabric modules

Some interface modules require high-speed switch fabric modules to operate (for example, NI-MLX-10Gx8-M and NI-MLX-10Gx8-D). If you are installing any of the following modules in your router, you must install high-speed switch fabric modules (if not already installed). For hardware installation instructions, refer to the *Brocade MLXe, NetIron MLX, and NetIron XMR Hardware Installation Guide*.

If you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules in your router, you must first upgrade the entire system to software R05.0.00c or later, and replace existing switch fabric modules with high-speed switch fabric modules. Be sure to remove all standard switch fabric modules **BEFORE** you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules in your router.

NOTE: Do not attempt to downgrade NI-MLX-10Gx8 modules or high-speed switch fabric modules to software versions older than R05.0.00. The modules will not operate with older software.

If you install -MLX-10Gx8 modules and do not replace the switch fabric modules with high-speed switch fabric modules, the NI-MLX-10Gx8 modules will not work. For 16-slot routers, you must also install high-speed fans. Refer to the *Brocade MLXe* and *NetIron MLX, and NetIron XMR Routers Hardware Installation Guide*.

To upgrade software and install high-speed switch fabric modules and NI-MLX-10Gx8 modules at the same time, first upgrade your router to R05.0.00c or later, then perform the following steps:

NOTE: Traffic may be briefly interrupted during an inline upgrade procedure.

1. Upgrade your router to R05.1.00. This upgrade must include all application, boot, and monitor files, and all management, interface, and switch fabric module FPGAs.

2. Restart your router.

3. Enter the **show version** command to confirm that the upgrade was successful.

4. Remove a standard switch fabric module (SFM).

5. Install a high-speed switch fabric module (hSFM) in the empty switch fabric slot.

6. To confirm that the new module is operating properly, enter the show module command.

   Repeat steps 4 through 6 to replace the remaining switch fabric modules with high-speed switch fabric modules.

7. Install a NI-MLX-10Gx8-M or NI-MLX-10Gx8-D module into an empty interface module slot.

8. To confirm that the module is operating properly, enter the show module command.

   Repeat steps 7 and 8 to install all remaining NI NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules.

Important upgrade memory requirement information

Before you begin the upgrade procedure, verify that you have enough available bytes free in the flash memory by entering the **dir** command:

Note: Lack of available flash memory is typically only seen in 32-slot devices.

```
NetIron# dir   <<<<<
Directory of /flash/

08/31/1908 13:26:14                  3 $$snmp_boots
08/06/2008 03:42:12                705 $$sshdsspub.key
07/30/2008 10:21:56              1,712 $$sslcert.key
08/09/2008 09:03:14            980,769 IMF.cfg
08/10/2008 12:49:09            981,804 IMF1.cfg
08/16/1908 06:38:47          2,663,857 ___mbridge
08/15/1908 09:21:34          2,663,857 ___mbridge.old   <<<<<<<<<<<<
08/20/1908 12:38:45                123 boot-parameter
08/21/1908 12:12:27            524,288 lp-monitor-0
08/27/1908 11:25:18          3,335,554 lp-primary-0
08/31/1908 06:13:15          3,304,730 lp-secondary-0
08/17/1908 14:10:29            422,393 monitor
08/27/1908 11:25:48          6,530,021 primary
08/31/1908 06:13:43          6,244,777 secondary
      08/31/1908 06:53:40            981,549 startup-config
```

```
                         15 File(s)        28,636,142 bytes
                          0 Dir(s)          2,097,152 bytes free
```

If necessary, you can delete the **mbridge.old** file to increase the available memory. Though unlikely, you may have to delete additional files for the upgrade to succeed. Contact Brocade technical support before removing additional files.

```
NetIron# delete___mbridge.old
```

Note: The file name **delete___mbridge.old** must contain *three* underscores.

After deleting the **mbridge.old** file, enter to **dir** command to verify that the **mbridge.old** file has been removed, and that there are enough bytes free to begin the upgrade.

```
        NetIron# dir   <<<<<
        Directory of /flash/

        08/31/1908 13:26:14                     3 $$snmp_boots
        08/06/2008 03:42:12                   705 $$sshdsspub.key
        07/30/2008 10:21:56                 1,712 $$sslcert.key
        08/09/2008 09:03:14               980,769 IMF.cfg
        08/10/2008 12:49:09               981,804 IMF1.cfg
        08/16/1908 06:38:47             2,663,857 ___mbridge

        <<<<<<<<<<<<<<<<<<<<mbridge.old file is removed
        08/20/1908 12:38:45                   123 boot-parameter
        08/21/1908 12:12:27               524,288 lp-monitor-0
        08/27/1908 11:25:18             3,335,554 lp-primary-0
        08/31/1908 06:13:15             3,304,730 lp-secondary-0
        08/17/1908 14:10:29               422,393 monitor
        08/27/1908 11:25:48             6,530,021 primary
        08/31/1908 06:13:43             6,244,777 secondary
        08/31/1908 06:53:40               981,549 startup-config

                      14 File(s)        25,972,285 bytes
                       0 Dir(s)          4,718,592 bytes free
```

You must also delete the **mbridge.old** file from the redundant management module, if one is installed. To access the redundant management module, enter the **switchover** command to make it the active management module.

```
        NetIron# switchover
        Are you sure? <enter 'y' or 'n'>
```

Enter **y**.

Once you have deleted the **mbridge.old** file and checked the available bytes free on the redundant management module, enter the **switchover** command again to make the original management module the active module. You are now ready to begin your upgrade.

CLI upgrade commands for R05.1.00

The following table lists the commands used to upgrade from R05.0.xx to R05.1.00.

Note: If you are upgrading using the combined images, you will only need to use a few of these commands.

Upgrade commands for R05.1.00

Combined application image command	
copy tftp image *<tftp_srvr>* **xm05100.bin {secondary] [delete-first]**	Combined management module and interface module application image. The **delete-first** option overwrites the primary flash images on management and interface modules automatically. The **secondary** option used with **delete-first** overwrites the secondary flash images automatically.
Management module image commands	
copy tftp flash *<tftp_srvr>* **xmr05100.bin pri**	Non-combined management module application, can be copied to secondary flash
copy tftp flash *<tftp_srvr>* **xmb05100.bin mon**	Management module monitor image
copy tftp flash *<tftp_srvr>* **xmprm05100.bin boot**	Management module boot image
Interface module image commands	
copy tftp lp *<tftp_srvr>* **xmlp05100.bin pri**	Non-combined interface module application, can be copied to secondary flash.
copy tftp lp *<tftp_srvr>* **xmlb05100.bin mon all**	Interface module monitor image
copy tftp lp *<tftp_srvr>* **xmlprm05100.bin boot all**	Interface module boot image
Management module MBRIDGE image commands	
copy tftp mbridge *<tftp_srvr>* **mbridge_05100.xsvf**	MBRIDGE image.
copy tftp mbridge *<tftp_srvr>* **mbridge32_05100.xsvf**	MBRIDGE32 image, for 32-slot devices only
Switch fabric and high-speed switch fabric module SBRIDGE and HSBRIDGE image commands	
copy tftp snm *<tftp_srvr>* **sbridge_05100.mcs sbridge all**	SBRIDGE image, for 32-slot devices only.
copy tftp snm *<tftp_srvr>* **hsbridge_05100.mcs hsbridge all**	HSBRIDGE image, for high-speed switch fabric modules only. (For 32-slot devices only.)
Interface module FPGA image commands	
copy tftp lp *<tftp_srvr>* **lpfpga05100.bin fpga-all all**	All interface module FPGA images combined.

copy tftp lp <*tftp_srvr*> **pbifsp2_05100.bin fpga-pbif all**	4x10 and 20x1 interface modules.
copy tftp lp <*tftp_srvr*> **xppsp2_05100.bin fpga-xpp all**	4x10 and 20x1 interface modules.
copy tftp lp <*tftp_srvr*> **xgmacsp2_05100.bin fpga-xgmac all**	4x10 interface modules only.
copy tftp lp <*tftp_srvr*> **pbifoc_05100.bin fpga-pbif all**	POS interface modules only.
copy tftp lp <*tftp_srvr*> **xppoc_05100.bin fpga-xpp all**	POS interface modules only.
copy tftp lp <*tftp_srvr*> **statsoc_05100.bin fpga-stats all**	All interface modules.
copy tftp lp <*tftp_srvr*> **pbifmrj_05100.bin fpga-pbif all**	48T interface modules only.
copy tftp lp <*tftp_srvr*> **xppmrj_05100.bin fpga-xpp all**	48T interface modules only.
copy tftp lp <*tftp_srvr*> **statsmrj_05100.bin fpga-stats all**	48T interface modules only.
copy tftp lp <*tftp_srvr*> **pbif8x10_05100.bin fpga-pbif all**	8x10 interface modules only.
copy tftp lp <*tftp_srvr*> **xpp8x10_05100.bin fpga-xpp all**	8x10 interface modules only.
copy tftp lp <*tftp_srvr*> **xgmacsp2_05100b.bin fpga-xpp all**	4x10 interface modules only.

Software upgrade procedures for Brocade MLXe, NetIron MLX, and NetIron XMR routers

The following sections contain specific procedures for upgrading your Brocade MLXe, NetIron MLX, and NetIron XMR router Multi-Service IronWare from R05.0.xx to R05.1.00.

Note: If you are upgrading from software versions older than R05.0.xx, refer to "Legacy Software Information".

Determining current software image versions

Before you upgrade your software, you should check the image versions currently installed to determine which ones need to be upgraded. If there are images on your system that are not compatible with R05.1.00 images, you will need to upgrade those images in addition to the basic required images.

To display image version information, enter the **show flash** or **show version** command. Compare the image versions to the compatible image version numbers in the table "Software images for R05.1.00."

To see output examples of the **show flash** and **show version** commands, refer to "Displaying flash information and "Displaying version information."

You should also check the installed images immediately after an upgrade to confirm that the upgrade was successful.

You should also verify that you have enough available flash memory to complete your upgrade. Refer to "Important upgrade memory requirements information."

Upgrading the combined IronWare Application Image on management modules

1. Place the new software images on an accessible TFTP server, or on a flash card inserted in slot 1 or 2 on the active management module.

2. Copy the new image from the TFTP server or the flash card to the flash memory on the management module by entering one of the following commands at the Privileged EXEC level of the CLI:

   copy tftp image *<tftp_srvr>* **xm05100.bin primary | secondary** [**delete-first**]

   copy slot1 | slot2 image *<ip-addr>* **xm05100.bin primary | secondary** [**delete-first**]

   The **primary** option copies the files to the primary image on the management module. The **secondary** option copies the files to the secondary image on the management module.

   The **delete-first** option automatically deletes the existing primary or secondary flash images before installing the new images.

3. Verify that the new image has been successfully copied to the specified destination by entering one of the following commands at the Privileged EXEC level of the CLI:

   show flash (if the destination was code flash)

   dir /*<path-name>***/** (if the destination was slot 1 or 2)

   Check for the primary or secondary image and the date and time that it was placed in the directory.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading the monitor image on a management module

To upgrade the monitor image on a management module, perform the following steps:

1. Place the new monitor image on an accessible TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.

2. Copy the new monitor image to the router by entering one of the following commands.

   copy tftp flash *<tftp_srvr>* **xmb05100.bin monitor** - copies the new monitor image from the TFTP server to flash memory on the management module.

   copy slot1 | slot2 flash xmb05100.bin monitor – copies the new monitor image from a flash card in slot 1 or slot 2 to flash memory on the management module.

3. Verify that the new monitor image has been successfully copied by entering one of the following commands at the Privileged EXEC level of the CLI:

   show flash

   dir /*<path-name>***/** (if the destination is slot 1 or 2)

   Check the monitor image version (xmb05100) and the date and time when the new image was built.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading the boot image on a management module

To upgrade the boot image on a management module, perform the following steps:

1. Place the new boot image on an accessible TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.

2.   Copy the new boot image to the router by entering one of the following commands.

copy tftp flash < *tftp_srvr* > **xmprm05100.bin boot** – copies the new boot image from the TFTP server to flash memory on the management module.

copy slot1 | slot2 flash xmprm05100.bin boot – copies the new boot image from a flash card to flash memory on the management module.

3.   Verify that the new boot image has been successfully copied by entering one of the following commands.

show flash

dir /<*path-name*>/ (if the destination is slot 1 or 2)

Check the boot and monitor image versions, and the date and time when the new images were built.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading the boot and monitor images on interface modules

It is recommended that you perform this upgrade from a PC or terminal that is directly connected to the Console port on the management module. You can also perform this procedure through a Telnet or SSHv2 session.

To upgrade monitor and boot images for all interface modules or a specified interface module perform the following steps.

1.   Place the new monitor and boot images on a TFTP server that the router can access, or on a flash card inserted in slot 1 or 2 of the management module.

2.   Copy the new monitor and boot images to all interface modules, or to a specified interface module by entering one of the following commands.

copy tftp lp <*tftp_srvr*> **xmlb05100.bin monitor all** |<*slot-number*> - copies the latest monitor image from the TFTP server to all interface modules or to a specified interface module.

copy tftp lp < *tftp_srvr* > **xmlprm05100.bin boot all** | <*slot-number*> - copies the latest boot image from the TFTP server to all interface modules, or to a specified interface module.

copy slot1 | slot2 lp <*ip-address*> **xmlb05100.bin monitor all** |<*slot-number*> - copies the latest monitor image from the flash card to all interface modules or to a specified interface module.

copy slot1 | slot2 lp <*ip-address*> **xmlprm05100.bin boot all** | <*slot-number*> - copies the latest boot image from the flash card to all interface modules, or to a specified interface module.

3.   Verify that the new images were successfully copied by entering the **show flash** command.

Check the monitor and boot image versions, and the date and time when the new images were built.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading interface modules using the combined FPGA image

To upgrade FPGA images on interface modules using the combined FPGA image, perform the following steps:

1.   Place the combined FPGA image on an accessible TFTP server, or on a flash card inserted in management module slot 1 or 2.

2.   Copy the bundled image from the TFTP server or flash card to all interface modules, or to a specific interface module by entering one of the following commands.

copy tftp lp <*tftp_srvr*> **lpfpga05100.bin fpga-all** [<*slot-num*> | **all**] [**force -overwrite** | <*module-type*>]

This command copies the combined FPGA image from a TFTP server

copy [**slot1**| **slot2**] **lp lpfpga05100.bin fpga-all** [*<slot-num>* | **all**] [**force -overwrite** | *<module-type>*]

This command copies the images from a flash card in slot 1 or slot 2 of the management module

The *<file-name>* variable specifies the file name of the bundled image for a specific software release.

The *<slot-num>* variable specifies the slot number.

The *<module-type>* variable specifies the interface module where the FPGA is to be upgraded.

The management module compares the copied FPGA versions to the images currently installed on all interface modules (the **all** option), or on a specified interface module (*<slot-num>*). If the FPGA images are identical, the download is aborted and a message is displayed:

```
Message: Copying 2nd image (PBIF - POS) to slot 1 skipped, same version exits. Use
"force-overwrite" if required.
```

The download will continue for interface modules that do not have matching FPGA images.

The **force-overwrite** option allows you to copy the FPGA image identical to the image currently installed. A warning message is not sent. The **force-overwrite** option can also be used for a specific module type.

Additional upgrade steps

The following sections describe additional upgrade steps that may be required for non-standard upgrades, or upgrades where you are not using the combined software images.

Upgrading MBRIDGE or MBRIDGE32 images on management modules

Note: This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to the table "Software images for R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR routers." If your router is running image versions that are not listed in the table, you will need to upgrade them.

To upgrade the MBRIDGE image on your management module, perform the following steps:

Note: If you are upgrading a 32-slot router, use the MBRIDGE32 image.

1. Place the new MBRIDGE image on an accessible TFTP server, or on a flash card inserted in slot 1 or 2 in the management module.

2. Copy the new MBRIDGE image to the router by entering one of the following commands.

    copy tftp mbridge *<tftp_srvr>* **mbridge_05100.xsvf** - copies the new image from the TFTP server to flash memory on the management module.

    copy slot1 | slot2 mbridge mbridge_05100.xsvf - copies the new image from a flash card to flash memory on the management module.

3. Verify that the new image has been successfully copied by entering one of the following commands at the Privileged EXEC level of the CLI:

    show flash

    dir /*<path-name>***/** (if the destination is slot 1 or 2)

    Check the mbridge image version and the date and time when the new image was built.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading the SBRIDGE image on switch fabric modules for 32-slot devices

Note: This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to the table "Software images for R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR routers." If your router is running image versions that are not listed in the table, you will need to upgrade them.

To upgrade the SBRIDGE image on switch fabric modules installed in a 32-slot device, perform the following steps:

1. Place the new SBRIDGE image on an accessible TFTP server, or on a flash card in slot 1 or 2 of the management module.

2. Copy the SBRIDGE image from the TFTP server or the flash card to all switch fabric modules or to a specified switch fabric module by entering the following command at the Privileged Exec level of the CLI:

3. **copy tftp snm** <*tftp_srvr* > **sbridge_05100.mcs sbridge all|**<*slot-number*>

    The **all** keyword copies the image to all switch fabric modules.

    The <slot number> copies the image to a specified switch fabric module.

4. Verify that the SBRIDGE image has been successfully copied by entering the **show version** command.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading the HSBRIDGE image on high-speed switch fabric modules for 32-slot devices

Note: This procedure is generally not required for a major software upgrade. To determine whether you need to upgrade these images, refer to the table "Software images for R05.1.00 for Brocade MLXe, NetIron MLX, and NetIron XMR routers." If your router is running image versions that are not listed in the table, you will need to upgrade them.

To upgrade the HSBRIDGE image on high-speed switch fabric modules installed in a 32-slot device, perform the following steps:

5. Place the new HSBRIDGE image on an accessible TFTP server, or on a flash card in slot 1 or 2 of the management module.

6. Copy the HSBRIDGE image from the TFTP server or the flash card to all high-speed switch fabric modules or to a specified high-speed switch fabric module by entering the following command:

    copy tftp snm <*tftp_srvr* > **hsbridge_05100.mcs hsbridge all|**<*slot-number*>

    The **all** keyword copies the image to all high-speed switch fabric modules.

    The <slot number> copies the image to a specified high-speed switch fabric module.

7. Verify that the HSBRIDGE image has been successfully copied by entering the **show version** command.

To upgrade other software images, refer to the appropriate upgrade section. When you have completed your upgrade, you must reboot the management module. Refer to "Rebooting the Management Module."

Upgrading individual FPGA images on interface modules

You can upgrade FPGA images individually on interface modules. To see which FPGA images are available, refer to Table 2.

Note: For a simplified FPGA image upgrade process, use the combined FPGA image for interface modules.

To upgrade FPGA images individually, perform the following steps.

1. Copy each FPGA image from the TFTP server or a flash card to all interface modules, or to a specified interface module by entering one of the following commands:

   copy tftp lp <*tftp_srvr*> <*image-name*> <*image-type*> **all** [<*module-type*>] [*force-overwrite*]

   copy tftp lp <*tftp_srvr*> <*image-name*> <*image-type*> <*chassis-slot-number*> [*force-overwrite*]

   copy slot1 | slot2 lp <*image-name*> <*image-type*> [<*module-type*>] [*force-overwrite*]

   copy slot1 | slot2 lp <*image-name*> <*image-type*> <*chassis-slot-number*> [*force-overwrite*]

   Specify the <image-name> of the fpga file you are copying, for example, **pbifsp2.bin**, **xppsp2.bin**, **statsoc.bin**, etc. For a complete list of individual fpga file names, refer to Table 2.

   If you specify the **<***module-type***>** (e.g., 4x10g), the router copies the images for that module only. If you specify **all** without a module-type, the system copies the appropriate images to the corresponding modules.

   The system compares FPGA versions being copied to those currently on the interface modules. If the images are identical, the download is aborted and the following warning message is displayed:

   ```
   Warning: same version of FPGA already exists on LP, no need to download FPGA again,
   use force-overwrite option to force download.
   ```

   If you use the **all** option, the system checks each interface module, and sends warning messages for Interface modules that have matching FPGA images. For interface modules that do not have matching FPGA images, the software proceeds with the download.

   If you use the **force-overwrite** option, an identical image is downloaded and the warning message is not sent.

2. The new FPGA images take effect when the management module is rebooted. You can also force the FPGA image to take effect on an interface module without rebooting the management module by "power cycling" the interface module using either of the following methods:

   - Turn the power off and on for the interface module using the **power-off lp** <*slot*> command followed by the **power-on lp** <*slot*> command.

   - Pull out and then reinsert the interface module.

   When the interface module boots, the FPGA Version Check utility confirms that compatible versions of the FPGA images are installed. At restart, or when the **show version** command is entered, the following information is displayed (this is an example only, versions may not be accurate).

   ```
   Valid PBIF Version = 3.21, Build Time = 11/11/2009 14:44:00
   Valid XPP Version = 6.02, Build Time = 1/31/2010 10:52:00
   Valid STATS Version = 0.07, Build Time = 12/11/2008 13:33:00
   ```

   If there is a problem with your FPGA upgrade, one of the following warnings will be displayed.

   ```
   WARN: Invalid FPGA version = 1.2, Build Time = 9/13/2005 13:20:0  <<<---
   ```

   This message indicates an FPGA version mismatch, or that one of the versions is not current.

   ```
   ERROR: failed to read FPGA versions from flash                   <<<---
   ```

   This message indicates that you have not completed a mandatory FPGA upgrade.

Rebooting the management module

When you complete your upgrade process, you must reboot the management module, which then reboots the interface modules.

To reboot the management module, enter one of the following commands:

reload (this command boots from the default boot source, which is the primary code flash)

boot system flash primary | secondary

During the management module reboot, the following synchronization events occur:

- The system compares the monitor, primary, and secondary images on a standby management module (if installed) to those on the active management module. If you have updated these images on the active module, the system automatically synchronizes the images on the standby module to match those on the active management module.

- If you copied the primary and secondary IronWare image to all interface modules using the **copy** command with the **all** keyword, the management module copied the image and stored it in flash memory under the names **lp-primary-0** or **lp-secondary-0**. By default, the system compares the IronWare images on the interface modules to the images on the management module to confirm that they are identical. (These IronWare images are stored on the management module only and are not run by the management or interface modules.) If the IronWare images are not identical, the system gives you the following options:

  - Replace the IronWare images in interface module flash memory with the images in the management module flash memory by entering the **lp cont-boot sync** *<slot-number>* command at the Privileged EXEC prompt.

  - To retain the IronWare images in the interface module flash memory, enter the **lp cont-boot no-sync <slot-number>** command at the Privileged EXEC prompt.

After the management module finishes booting, perform the following steps:

1. Enter the **show module** command, and verify that the status of all interface modules is CARD_STATE_UP.

2. Enter the **show version** command, and verify that all management and interface modules are running the new software image version.

Note: If an interface module is in a waiting state or is running an older software image, you may have forgotten to enter the **lp cont-boot sync** *<slot-number>* command at the Privileged EXEC prompt.

Performing a Hitless OS upgrade

Note: Hitless upgrades are supported for upgrades within a major release (for example, 05.1.00 to 05.1.00a) but are not supported for upgrades from one major release to another (for example 05.0.00 to 05.1.00.)

Some features and protocols are not supported for hitless upgrade. Before you perform a hitless upgrade, refer to "Hitless OS Upgrade" for more information.

A Hitless OS Upgrade loads from the primary and secondary images on the management modules.

To do a Hitless OS Upgrade, perform the following steps:

1. Copy the Multi-Service IronWare software images to the primary and secondary flash on the active and standby management modules and on interface modules.

2. Set up a console connection to both the active and standby management modules. These connections can be serial console sessions or sessions established through Telnet or SSH.

3. Enter the **hitless-reload** command at the console of the active management module.

   hitless-reload mp [primary | secondary] | lp [primary | secondary]

   The **mp** parameter specifies that the image will be copied to the *management module.*

   The **lp** parameter specifies that the image will be reloaded to the *interface module.*

Performing an image coherence check

When you enter the **reload-check** command, Multi-Service IronWare software performs a coherence check to ensure that compatible versions of the software are installed on management and interface modules, and that all interface module FPGAs are compatible with the current software version. If incompatible images are discovered, a warning message is sent.

The image coherence check is performed in the following sequence:

1. Check management module and interface module application images for compatibility

    a. Checks for compatibly of interface module application images on management and interface modules.

    b. Checks for compatibly of interface module monitor images on management and interface modules.

2. Checks the interface module monitor image on the management module and all interface modules

3. Checks the management module monitor image for compatibility with the management module application image.

4. Checks the interface module monitor image for compatibility the management and interface module application images.

5. Checks all interface module FPGAs for compatibility with the application image. FPGAs include CPP, PBIF, XGMAC, STATS, XPP-OC, PBIF-OC, STATS-OC.

If step 1 does not succeed, verification is stopped and a warning is issued. If step 1 succeeds, the rest of the checks are conducted in parallel.

Performing a coherence check without a reload

Enter the **reload-check** command to perform a coherence check *without* performing a reload, as shown in the following example:

```
NetIron# reload-check
Checking for coherence...

Warning: The new LP PBIF-8X10 FPGA will not be compatible with the new LP 3 application.

Warning: The new LP XPP-8X10 FPGA will not be compatible with the new LP 3 application.
Done.
NetIron#
```

Error messages generated by the coherence check

The following error messages are generated if a coherence check fails:

```
Warning: Image coherence check skipped due to insufficient info: Invalid active LP
flash images in Primary/Secondary.

Warning: Image coherence check skipped due to insufficient info: Invalid active MP
flash images in Primary/Secondary.

Warning: Image coherence check skipped due to insufficient inf: MP/LP not booting
from flash.

Warning: Image coherence check skipped due to failure to communicate with LP.
```

NOTE: If interface modules are in interactive mode, or the system is unable to communicate with the interface modules, the system sends the following warning message: `Can't check LP for coherence.`

Displaying image versions for Brocade MLXe, NetIron MLX, and NetIron XMR devices

The following sections describe how to display software image version information for Brocade MLXe, NetIron MLX, and NetIron XMR routers, using the **show flash** or **show version** commands.

Using the show flash command

You can display the images stored in flash memory using the **show flash** command.

Note: This example is for illustration only and may not reflect current image version information.

Output from the **show flash** command resembles this example.

```
NetIron# show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Active Management Module (Left Slot)
Code Flash - Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 5.1.0T163, Size 6986803 bytes, Check Sum 74d5
    Compiled on Sep 16 2010 at 17:49:56 labeled as xmr05100
  o IronWare Image (Secondary)
    Version 5.1.0T163, Size 6984593 bytes, Check Sum d570
    Compiled on Aug 17 2010 at 16:13:36 labeled as xmr05100b1
  o LP Kernel Image (Monitor for LP Image Type 0)
    Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
    Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
  o LP IronWare Image (Primary for LP Image Type 0)
    Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
    Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
  o LP IronWare Image (Secondary for LP Image Type 0)
    Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
    Compiled on Aug 18 2010 at 17:39:16 labeled as xmlp05100b1
  o Monitor Image
    Version 5.1.0T165, Size 524053 bytes, Check Sum 70b1
    Compiled on Aug 11 2010 at 14:06:30 labeled as xmb05100
  o Startup Configuration
    Size 12652 bytes, Check Sum dd86
    Modified on 21:57:42 Pacific Thu Sep 16 2010

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 5.1.0T165, Size 524038 bytes, Check Sum 59a3
    Compiled on Aug 11 2010 at 14:06:58 labeled as xmprm05100
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Standby Management Module (Right Slot)
Code Flash: Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 5.1.0T163, Size 6986803 bytes, Check Sum 74d5
    Compiled on Sep 16 2010 at 17:49:56 labeled as xmr05100
  o IronWare Image (Secondary)
    Version 5.1.0T163, Size 6984593 bytes, Check Sum d570
    Compiled on Aug 17 2010 at 16:13:36 labeled as xmr05100b1
  o LP Kernel Image (Monitor for LP Image Type 0)
    Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
    Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
  o LP IronWare Image (Primary for LP Image Type 0)
    Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
    Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
  o LP IronWare Image (Secondary for LP Image Type 0)
```

```
          Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
          Compiled on Aug 18 2010 at 17:39:16 labeled as xmlp05100b1
    o Monitor Image
          Version 5.1.0T165, Size 524053 bytes, Check Sum 70b1
          Compiled on Aug 11 2010 at 14:06:30 labeled as xmb05100
    o Startup Configuration
          Size 12652 bytes, Check Sum dd86
          Modified on 14:15:27 Pacific Fri Sep 17 2010


Boot Flash: Type AM29LV040B, Size 512 KB
    o Boot Image     Version 5.1.0T165, Size 524038 bytes, Check Sum 59a3
          Compiled on Aug 11 2010 at 14:06:58 labeled as xmprm05100
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 4
Code Flash: Type MT28F640J3, Size 16 MB
    o IronWare Image (Primary)
          Version 5.1.0T177, Size 4950936 bytes, Check Sum d368
          Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
    o IronWare Image (Secondary)
          Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
          Compiled on Aug 18 2010 at 17:39:16 labeled as xmlp05100b1
    o Monitor Image
          Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a
          Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
Boot Flash: Type AM29LV040B, Size 512 KB
    o Boot Image
          Version 5.1.0T175, Size 492544 bytes, Check Sum 6c2b
          Compiled on Aug 11 2010 at 14:07:20 labeled as xmlprm05100
FPGA Version (Stored In Flash):
 PBIF Version = 3.24, Build Time = 8/4/2010 14:57:00

 XPP Version = 6.03, Build Time = 2/18/2010 16:38:00

 STATS Version = 0.08, Build Time = 2/18/2010 16:30:00


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 6
Code Flash: Type MT28F640J3, Size 16 MB
    o IronWare Image (Primary)
          Version 5.1.0T177, Size 4950936 bytes, Check Sum d368

          Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
    o IronWare Image (Secondary)
          Version 5.1.0T177, Size 4947628 bytes, Check Sum 3f13
          Compiled on Aug 18 2010 at 17:39:16 labeled as xmlp05100b1
    o Monitor Image
          Version 5.1.0T175, Size 493244 bytes, Check Sum fd4a

          Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
Boot Flash: Type AM29LV040B, Size 512 KB
    o Boot Image
          Version 5.1.0T175, Size 492544 bytes, Check Sum 6c2b
          Compiled on Aug 11 2010 at 14:07:20 labeled as xmlprm05100
FPGA Version (Stored In Flash):
 PBIF Version = 3.22, Build Time = 2/5/2010 14:43:00

 XPP Version = 6.04, Build Time = 2/3/2010 14:39:00

 XGMAC Version = 0.13, Build Time = 2/3/2010 14:42:00


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
All show flash done
```

show version

Enter the **show version** command to display version information for your router. For detailed descriptions of the fields shown in the output from this command, refer to the *Brocade MLXe, NetIron MLX, and NetIron XMR Hardware Installation Guide.*

Note: This example is for illustration only and may not reflect current image version information.

```
NetIron# show version
System Mode: MLX
Chassis: NetIron 8-slot (Serial #:        GOLD,  Part #: 35549-000C)
NI-X-SF  Switch Fabric Module 1 (Serial #: PR23050271,  Part #: 31523-100A)
FE 1: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
NI-X-SF  Switch Fabric Module 2 (Serial #: SA21091164,  Part #: 35523-302A)
FE 1: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
NI-X-SF  Switch Fabric Module 3 (Serial #: SA21091204,  Part #: 35523-302A)
FE 1: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
==========================================================================
SL M2: NI-MLX-MR Management Module Active (Serial #: SA21091472, Part #: 35524-103C):
Boot: Version 5.1.0T165 Copyright(c)1996-2009 Brocade Communications Systems,Inc.
Compiled on Aug 11 2010 at 14:06:58 labeled as xmprm05100
 (524038 bytes) from boot flash
Monitor: Version 5.1.0T165 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:06:30 labeled as xmb05100
 (524053 bytes) from code flash
IronWare: Version 5.1.0T163 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Sep 16 2010 at 17:49:56 labeled as xmr05100
 (6986803 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 32
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
1024 MB DRAM
Active Management uptime is 1 minutes 28 seconds
==========================================================================
SL M1: NI-MLX-MR Management Module Standby (Serial #: SA21091421, Part #: 35524-103C):
Boot: Version 5.1.0T165 Copyright (c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:06:58 labeled as xmprm05100
 (524038 bytes) from boot flash
Monitor: Version 5.1.0T165 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:06:30 labeled as xmb05100
 (524053 bytes) from code flash
IronWare: Version 5.1.0T163 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Sep 16 2010 at 17:49:56 labeled as xmr05100
 (6986803 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 32
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
1024 MB DRAM
Standby Management uptime is 53 seconds
==========================================================================
SL 4:NI-MLX-1Gx48-T 48-port 10/100/1000Base-T MRJ21 Module(Serial#: SA05091472,Part#:
35663-20EA)
Boot: Version 5.1.0T175 Copyright(c) 1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:07:20 labeled as xmlprm05100
 (492544 bytes) from boot flash
Monitor: Version 5.1.0T175 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
 (493244 bytes) from code flash
```

```
IronWare: Version 5.1.0T177 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
 (4950936 bytes) from Primary
FPGA versions:
Valid PBIF Version = 3.24, Build Time = 8/4/2010 14:57:00


Valid XPP Version = 6.03, Build Time = 2/18/2010 16:38:00


Valid STATS Version = 0.08, Build Time = 2/18/2010 16:30:00


BCM56502GMAC 0
BCM56502GMAC 1
666 MHz MPC 8541 (version 8020/0020) 333 MHz bus
512 KB Boot Flash (AM29LV040B), 16 MB Code Flash (MT28F640J3)
1024 MB DRAM, 8 KB SRAM, 0 Bytes BRAM
PPCR0: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
PPCR1: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
LP Slot 4 uptime is 58 seconds
============================================================================
SL 6: NI-MLX-10Gx4 4-port 10GbE Module (Serial #: SA12090950, Part #: 35600-202D)
Boot: Version 5.1.0T175 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:07:20 labeled as xmlprm05100
 (492544 bytes) from boot flash
Monitor: Version 5.1.0T175 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Aug 11 2010 at 14:07:42 labeled as xmlb05100
 (493244 bytes) from code flash
IronWare: Version 5.1.0T177 Copyright(c)1996-2009 Brocade Communications Systems, Inc.
Compiled on Sep 16 2010 at 17:55:24 labeled as xmlp05100
 (4950936 bytes) from Primary
FPGA versions:
Valid PBIF Version = 3.22, Build Time = 2/5/2010 14:43:00


Valid XPP Version = 6.04, Build Time = 2/3/2010 14:39:00


Valid XGMAC Version = 0.13, Build Time = 2/3/2010 14:42:00


X10G2MAC 0
X10G2MAC 1
666 MHz MPC 8541 (version 8020/0020) 333 MHz bus
512 KB Boot Flash (AM29LV040B), 16 MB Code Flash (MT28F640J3)
512 MB DRAM, 8 KB SRAM, 286331153 Bytes BRAM
PPCR0: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
PPCR1: 768K entries CAM, 8192K PRAM, 2048K AGE RAM
LP Slot 6 uptime is 59 seconds
============================================================================
All show version done
```

Legacy software upgrade information for Brocade MLXe, NetIron MLX, and NetIron XMR devices

The following sections contain information and procedures to use if you are upgrading from older software versions, or downgrading to older software versions. Contact Technical Support if you do not find the information you need in these sections.

General legacy downgrade and upgrade considerations

- If you are upgrading from a release earlier than 3.8.00c to 3.9.00 and later, you should delete the **mbridge.old** file from the flash memory of both active and standby management modules before starting the upgrade process. The upgrade may fail if this procedure is not followed.

- If you are upgrading from R04.1.00 or earlier, your management module flash may not contain enough memory to complete the upgrade. It is recommended that you delete the primary image files from the management module and interface modules before attempting to upgrade. For information on how to delete the necessary files from your flash memory, refer to "Upgrading to R05.00b from R04.1.00 and earlier."

- When upgrading to R04.0.00 and later there will be changes to the ifIndex allocations, port MAC addresses, and QoS Priorities for NI-MLX-1Gx48-T-A modules.

- The combined FPGA image will not work for devices with modules running R04.1.00. For these devices, you must upgrade FPGA images individually. For a list of FPGA names, refer to "FPGA images for Multi-Service IronWare R05.0.00c." For detailed information about how to copy FPGAs, refer to "Upgrading the FPGA image upgrade."

- Routers with POS interface modules should not be downgraded to Multi-Service IronWare software releases earlier than R03.4.00.

- NetIron MLX-32 and NetIron XMR 32000 routers should not be downgraded to Multi-Service IronWare software releases earlier than R03.6.00.

- Downgrading from R04.1.00 to an earlier release of the software can impact IPv6 routing. IPv6 routing is enabled by default in R04.1.00 and therefore does not appear in the configuration. If you are downgrading from R04.1.00 to an earlier version of the software and want IPv6 routing to be enabled, you must add the line "ipv6 unicast-routing" to the configuration.

- NetIron XMR 32000 and MLX-32 routers can operate with interface modules that are running older software versions. For more information about running older software in a 32-slot chassis, refer to *Multi-Service IronWare Software Release 04.0.01 for Brocade NetIron XMR and NetIron MLX Release Notes v1.0*.

Upgrading to R04.0.00 and later

When upgrading to R04.0.00 and later, and installing NI-MLX-1Gx48T modules, you must also change the following items:

- ifIndex allocation
- Port MAC address change
- QoS priorités for NI-MLX-1Gx48-T modules

These changes are described in the following sections.

ifIndex allocation

The SNMP Management Information Base (MIB) uses the Interface Index (ifIndex) to assign a unique value to each port on a module or slot. Beginning with R04.0.00, the number of indexes that can be assigned per module is 20, 40, or 64, depending on the number of ports on the module. When upgrading to R04.0.00, consider the following:

- If you are running R03.9.00 or earlier and you will be installing the NI-MLX-1Gx48-T module on your device, you must configure the maximum ifIndex per module to 64. **You must change the ifIndex allocation before installing the NI-MLX-1Gx48-T module**; otherwise, the module remains in the Offline state.

- If you are running R03.9.00 or earlier and you will *not* be installing the NI-MLX-1Gx48-T module, you do not need to change your ifIndex allocation scheme. The current definition is maintained. The maximum ifIndex per module can remain at 20 or 40.

- If you have a new device (no previous software installed), and you will be installing an NI-MLX-1Gx48-T module, you **must** configure the maximum ifIndex per module to 64; otherwise, the module remains in the Offline state.

- If you have a new device (no previous software installed), and will not be installing an NI-MLX-1Gx48-T module, it is recommended that you configure the maximum ifIndex per module to 64 to avoid future ifIndex problems if you decide to install an NI-MLX-1Gx48-T module in the future.

Port MAC address change

Beginning with R04.0.00, the MAC address assigned to each port may change to accommodate a greater number of ports per module. The MAC address ports allocated for each module has increased from 20 to 48.

QoS priorities for NI-MLX-1Gx48-T modules

Beginning with R04.0.00, you can configure more ports in the system by changing the QoS per-port priorities from 8 to 4. This enables the device to support 2016 ports using 4 priorities per port.

Upgrading routers running R04.1.00 and earlier to R05.1.00

To upgrade a router running R04.1.00 and earlier to R05.1.00, you must first delete the primary and lp-primary-0 images, using these steps.

1. Before you copy the R05.1.00 image to the primary flash on the management module, first delete the primary and lp-primary-0 images from the primary flash using these commands:

   ```
   MP# del primary
   MP# del lp-primary-0
   ```

   Note: If the primary flash contains additional files not related to the software upgrade, it is recommended that you also delete these files.

2. Before you copy the R05.1.00 image to the primary flash on the interface modules, delete the existing **primary** image by entering commands similar to the following.

   ```
   Router1# rconsole 2
   Remote connection to LP slot 2 established
   Press CTRL-X or type 'exit' to disconnect it
   LP-2>en
   No password has been assigned yet...
   LP-2# delete primary
   ```

3. Copy the combined IronWare applications image to the primary flash on the management module.

4. Copy the R05.0.00c boot and monitor images to the primary flash on the management module and interface modules.

5. Copy the mbridge image to the primary flash on the management module. Refer to "Upgrading the MBRIDGE FPGA image on a management module."

NOTE: If there is a file on the management module named *mbridge-old*, delete this file.

6. For 32-slot devices, copy the sbridge image to each switch fabric module. This step is only necessary if you are not already running sbridge image 6. Refer to *"Upgrading the SBRIDGE image."*

Note: If you are currently running R04.1.00 or 04.1.00a, *DO NOT* upgrade to sbridge image 6. When loading the sbridge image from a system running 4.1.00 or 4.1.00a, the image on the switch fabric modules may become corrupted.

7. Copy all FPGA images individually (the bundled FPGA image upgrade feature will not work for devices running R04.1.00a and older). For a list of FPGA names, refer to *"Image files in Multi-Service IronWare R05.0.00c for the Brocade MLXe, NetIron MLX, and NetIron XMR series"*. For detailed information about how to copy FPGAs, refer to *"Upgrading FPGA images"*.

8. Perform a coherence check. For detailed instructions, refer to *"Performing a Coherence Check."*

Legacy image versions for Multi-Service IronWare software

You must have the correct FPGA images loaded on your router to run the software. The following tables list the FPGA versions required to run the listed software releases.

NOTE: The FPGA images described here are for use with Brocade MLXe, NetIron MLX, and NetIron XMR series routers only. These images will not work for other NetIron platforms.

FPGA Image Files for Management Modules in 4, 8, and 16-slot routers

Software release	FPGA Image	Compatible version	Module supported
04.0.00 through 04.1.xx	MBRIDGE	21	Management module
05.0.00 through 05.0.00c		32	Management module

FPGA Image Files for Management Modules in 32-slot routers

Software release	FPGA Image	Compatible version	Module supported
04.0.00 through 04.1.xx	MBRIDGE32	21	Management module
05.0.00 through 05.0.00c		32	Management module

FPGA Image Files for Switch Fabric Modules (32-slot devices only)

Software release	FPGA image	Compatible version	Module supported
04.0.00 through 05.0.00c	SBRIDGE	6	Switch fabric module (32-slot devices only)

FPGA Image Files for High-Speed Switch Fabric Modules

Software release	FPGA image	Compatible version	Module supported
05.0.00 through 05.0.00c	HSBRIDGE	16	High-speed switch fabric module

Upgrading software on NetIron CER and NetIron CES devices

This section describes how to upgrade software on NetIron CER and NetIron CES devices. The procedures described are identical for both models, except where indicated.

R05.1.00 image files for NetIron CER and NetIron CES devices

The following software image files are available for Multi-Service IronWare R05.1.00 for NetIron CES 2000 series and NetIron CER 2000 series devices.

NOTE: The software described in this section applies only to NetIron CER and NetIron CES devices. You cannot use this software on other Brocade devices.

NetIron CER and NetIron CES image file names for R05.1.00

Image Type	Function	Image Name
Boot	Bootstrap	ceb05100.bin
Monitor	Image Handling Memory Init	ceb05100.bin
Multi-Service IronWare	Application OS	ce05100.bin

NOTE: NetIron CES and NetIron CER devices use the same file image for boot and monitor images.

Upgrading CES and NetIron CER devices from R05.0.xx to R05.1.00

Upgrading Multi-Service IronWare software for NetIron CES and NetIron CER devices usually requires that you upgrade the Multi-Service IronWare image only. Boot and monitor images should only be upgraded if you are specifically instructed to do so in the relevant release notes.

This upgrade requires the following steps:

1. Upgrade the Multi-Service IronWare image.

2. Reboot the NetIron CES or NetIron CER device.

In most cases, these steps are all that is required. If you are directed to upgrade monitor or boot images, follow the procedures described in "Upgrading monitor and boot images", then reboot the NetIron CES or NetIron CER device.

Determining current image versions for NetIron CER and NetIron CES devices

Before you upgrade the images on a NetIron CES or NetIron CER device, you should check the image versions already installed to determine which ones need to be upgraded. You should also check the versions after you complete your upgrade to confirm that the upgrade was successful. Use the **show flash** and **show version** commands to display this information.

Compare the image versions in the output of these commands to the versions listed in the table "NetIron CER and NetIron CES image file names for R05.1.00." Upgrade any image versions that do not match the table.

show flash

You can display flash memory information by entering the **show flash** command as shown in the following example. To see which boot, monitor, and IronWare image versions and file names are appropriate for this release, refer to "Image files in Multi-Service IronWare R05.1.00 for NetIron CER and NetIron CES devices."

Note: This example is for illustration only and may not reflect current image version information.

```
NetIron CER# show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Code Flash - Type MT28F256J3, Size 64 MB
  o IronWare Image (Primary)
    Version 5.1.0T183, Size 12219543 bytes, Check Sum 259b
    Compiled on Sep 10 2010 at 13:46:44 labeled as ce05100b344
  o IronWare Image (Secondary)
    Version 5.1.0T183, Size 12217995 bytes, Check Sum c28b
    Compiled on Sep 15 2010 at 18:12:56 labeled as ce05100b356
  o Monitor Image
    Version 5.1.0T185, Size 441454 bytes, Check Sum 89ba
    Compiled on Jun 21 2010 at 18:14:42 labeled as ceb05100b141
  o Startup Configuration
    Size 878 bytes, Check Sum 1181
    Modified on 00:18:52 GMT+00 Fri Sep 17 2010

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 5.1.0T185, Size 441454 bytes, Check Sum 89ba
    Compiled on Jun 21 2010 at 18:14:42 labeled as ceb05100b141
```

show version

You can display version information for a NetIron CES 2000 or NetIron CER 2000 series device using the **show version** command as shown in the following. The example below is for illustration only and may not reflect current image version information. Version information has been highlighted in this example

```
NetIron CER# show version
System: NetIron CER (Serial #: Not Exist,  Part #: Not Exist)
License: ADV_SVCS_PREM (LID: )
Boot      : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jun 21 2010 at 18:14:42 labeled as ceb05100b141
 (441454 bytes) from boot flash
Monitor   : Version 5.1.0T185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jun 21 2010 at 18:14:42 labeled as ceb05100b141
 (441454 bytes) from code flash
IronWare : Version 5.1.0T183 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Sep 10 2010 at 13:46:44 labeled as ce05100b344
 (12219543 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000d
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 64 MB Code Flash (MT28F256J3)
2048 MB DRAM
Daughter Board: Serial #: SA24090135, Part #: Not Exist
System uptime is 2 minutes 11 seconds
CER-OLD#
```

Upgrading monitor and boot images on a NetIron CES or NetIron CER device

In most cases, when upgrading from one major release to another, it is not necessary to upgrade the boot and monitor images for NetIron CES and CER devices, unless you are specifically instructed to do so. For R05.1.00, it is not necessary to upgrade the boot image.

To upgrade monitor and boot images, perform the following steps:

1. Place the new monitor and boot images on an accessible TFTP server.

2. Copy the new monitor and boot images to the switch using one of the following commands

   copy tftp flash <*tftp_srvr*> **ceb05100.bin monitor**

   copy tftp flash <*tftp_srvr*> **ceb05100.bin boot**

3. Verify that the new monitor and boot images have been successfully copied to flash or slot 1 or 2 by entering one of the following commands at the Privileged EXEC level of the CLI:

   show flash

   dir /<*path-name*>**/**

   Verify that the new boot image and monitor images have been installed.

4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed your upgrade, you must reboot the switch for the upgrade to take effect.

Upgrading the application image for NetIron CES and NetIron CER devices

To upgrade the Multi-Service IronWare application image (primary or secondary) for a NetIron CES or NetIron CER device, (primary or secondary), perform the following steps:

1. Copy the new Multi-Service IronWare image from the TFTP server to the flash memory on the management module, by entering the following command at the Privileged EXEC level of the CLI:

   copy tftp flash <*tftp-srvr*> *ce***05100.bin primary | secondary**

2. Verify that the new Multi-Service IronWare image has been successfully copied by entering one of the following commands at the Privileged EXEC level of the CLI:

show flash (if the destination was code flash)

dir /<*path-name*>/

Verify that the new primary and secondary image has been installed.

5. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed your upgrade, you must reboot the switch for the upgrade to take effect.

Legacy software upgrade information for NetIron CER and NetIron CES devices

The following considerations apply to legacy software upgrades for NetIron CER and NetIron CES devices.

- For upgrades from R04.1.00 to R05.0.00, and from R05.0.00 to R05.1.00, it is not necessary to upgrade the boot image.

- NetIron CER devices should not be downgraded to pre-R04.1.00a software versions.

Loading and saving configuration files

For easy configuration management, the router supports both the download and upload of configuration files between the router and a TFTP server on the network. You can also copy the startup configuration file locally between the management module's code flash and a PCMCIA flash card inserted in management module slot 1 or 2.

You can upload either the startup configuration file or the running configuration to the TFTP server, code flash, or a flash card for backup and use in booting the system.

- **Startup configuration file** – This file (startup-config) contains the configuration information that is currently saved in the NetIron CES and NetIron CER series code flash. To display this file, enter the show configuration command at any CLI prompt.

- **Running configuration** – This active configuration is in the system RAM but not yet saved to code flash. These changes could represent a short-term requirement or general configuration change. To display this configuration, enter the show running-config or write terminal command at any CLI prompt.

Each device can have one startup configuration file and one running configuration. The startup configuration file is shared by both flash modules. The running configuration resides in DRAM.

Configuring file size for startup and running configuration

The system allocates 8 MB of contiguous memory per session (console, TELNET, SSH) for processing different configuration commands, such as **show run**, **config terminal**, and **copy tftp run**. In a low memory state, memory is generally fragmented resulting in a failure to allocate contiguous memory to support the session. We now pre-allocate one configuration buffer so that at least one CLI session will remain operational even in low memory condition.

NOTE: The low memory condition is not a normal operating condition, and may indicate scaling the network beyond system max limits. However, this feature ensures that one CLI session remains operational so that the user can take suitable actions to recover from the condition.

To specify a configuration file size for both startup and running configuration, enter the following command:

```
NetIron(config)# system-max
```

Syntax: [no] system-max [config-file-size *<decimal>*]

By default, **no system-max parameter** is configured.

The **config-file-size** option specifies the configuration file size for processing various commands.

The **decimal** parameter specifies the range supported for configuring file size. The minimum configuration is 2 MB, and the maximum is 16 MB. If the file size is not configured, the default size of 8 MB is used.

NOTE: It is strongly recommended that you use the default size (8 MB) when configuring file size.

When you enter the **system-max** command, with the config-file-size parameter included, the following additional information is displayed:

```
NetIron(config)# system-max config-file-size 2097152
Reload required. Please write memory and then reload or power cycle.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
Replacing the Startup Configuration with the Running Configuration
```

NOTE: You must enter the **write memory** command and restart the system for this command to take effect.

Replacing the startup configuration with the running configuration

After you make configuration changes to the active system, you can save the changes to flash memory, which replaces the existing startup configuration with the new running configuration.

To replace the startup configuration with the new running configuration, enter the **write memory** command.

```
 NetIron# write memory
```

Retaining the current startup configuration

After making configuration changes to the active system, if you have not executed a **write memory** command and you decide you don't want to save the changes, enter the **reload** command to return to the current startup configuration.

```
 NetIron# reload
```

If the system detects differences between the running and startup configurations, it prompts you as follows:

```
Are you sure? (enter 'y' or 'n'):
```

Enter **y**, and press the **Enter** key.

Copying a configuration file to or from a TFTP server

To copy the startup-config or running-config file to or from a TFTP server, use one of the following methods.

NOTE: You can name the configuration file when you copy it to a TFTP server. However, when you copy a configuration file from the server to a device, the file is always copied as "startup-config" or "running-config", depending on which type of file you saved to the server.

To copy configuration files to or from a TFTP server, enter one of the following commands:

- **copy startup-config tftp** *<ip-address>* *<filename>* – Use this command to upload a copy of startup-config from the device to a TFTP server.

- **copy running-config tftp** *<ip-address>* *<filename>* – Use this command to upload a copy of the running configuration from the device to a TFTP server.

- **copy tftp startup-config** *<ip-address>* *<filename>* – Use this command to download a copy of the startup-config from a TFTP server to the device.

copy tftp running-config <*tftpip -address*> <*filename*> [**overwrite**] – Use this command to download the access-list to the running-configuration. The new access-list is then appended to the current running configuration of the NetIron router.

Making local copies of the startup configuration file

You can copy the startup-config file in flash memory to a TFTP server or to a PCMCIA flash card inserted in management module slot 1 or 2.

For example, to make a backup copy of the startup-config file and save the backup file to a TFTP server, enter a command such as the following at the Privileged EXEC level in the CLI:

```
NetIron# copy startup-config tftp 10.28.40.21 startup-config.bak
```

Syntax: copy startup-config tftp <*ip-address*> <*dest-file-name*>

The <*ip-address*> variable specifies the IP address of the TFTP server that you want to save the startup configuration to.

The <*dest-file-name*> specifies the name of the file you copied to a new destination.

For example, to make a backup copy of the startup-config file and save the backup file on a flash card in slot 2, enter a command such as the following at the Privileged EXEC level in the CLI:

```
NetIron# copy startup-config slot2 /backups/startup-config.bak
```

Syntax: copy startup-config [**slot1** | **slot2**] [/<*dest-dir-path*>]/<*dest-file-name*>

Specify the <*dest-dir-path*> parameter to copy the source file to a file system that does not have current management focus.

The <*dest-file-name*> specifies the name of the file you copied to a new destination.

Hitless OS upgrade

You can upgrade Multi-Service IronWare software using the Hitless OS upgrade feature with no loss of service or disruption in the most functions and protocols. During the Hitless OS upgrade process, all ports and links remain operational. The following table lists supported and unsupported protocols for Hitless OS upgrade.

Supported for Hitless OS upgrade	Not supported for Hitless OS upgrade

TOS-based QoS
Layer 2 switching
Layer 2 protocols:
   MRP
   STP
   RSTP
   VSRP
Layer 3 protocols
   IGMP
   PIM
   OSPF
   BGP
   IS-IS
Static IP routes
Layer-3 forwarding
GRE tunnels
ACLs (the following ACLS continue to function but ACL counters are reset)
   Layer 2 ACLs
   IPv4 ACLs
   IPv6 ACLs
   IP Receive ACLs
   IPv4 and Layer-2 ACL-based traffic policing Traffic policing
UDLD
LACP
BFD
802.1ag over VLANs
	802.1s
	All MPLS features
	IPv4 and IPv6 multicast snooping
	IPv4 and IPv6 multicast routing
	VLAN translation
	Policy-based routing
	FPGA upgrades
	POS
	Unicast
	VRRP and VRRP-E
	All VPN features
	MCT (Multi-chassis trunking)
	Network management to the device:
	  SSH
	  Telnet
	  SNTP
	  HTTP/HTTPS
	  sFlow (interface modules only)
	  Ping
	  Traceroute
	  Syslog messages are cleared
	  SNMP and SNMP trap
	  DNS
	  DHCP
	  AAA
	ERP (G.8032)
	Management VRF

NOTE: Services not supported for Hitless OS Upgrade may encounter disruptions when the management and interface modules are restarted, but will resume normal operation once the modules are again operational.

Considerations when using Hitless OS upgrade

Consider the following information when using this feature:

- Both active and standby management modules must be installed to use this feature.

- To avoid disruptions of Layer-3 traffic to OSPF or BGP routes, OSPF Non-stop routing or OSPF Graceful Restart and BGP Graceful Restart features must be configured on the router. In addition, OSPF neighbors of the router must have OSPF Graceful Restart Helper enabled if OSPF Graceful Restart is enabled.

- To avoid disruptions of IPv4 Layer 3 multicast traffic, the unicast routing protocol for multicast RPF routes must be either Non-Stop routing- or Graceful Restart-capable and enabled .

- The time required for the hitless upgrade process ranges from 1 to 10 minutes, depending on the size of the MAC table and the routing table, and the number of OSPF and BGP neighbors. Router configuration is unavailable during the entire hitless upgrade process. The message "**—SW Upgrade In Progress - Please Wait—**" is displayed at the console if configuration is attempted. Operational command of the router is allowed during the upgrade process.

- Because the active management module becomes the standby management module during the hitless upgrade process, you will need a connection to the console interface on both management modules.

- When they are reset, management and interface modules are unable to send and receive packets. Once the management and interface modules are again operational, modules can send and receive packets, even before the hitless upgrade process is complete.

- Router configuration cannot be changed during the hitless upgrade process.

- System-max parameter changes (or other configuration changes that require a system reload, such as "cam-mode" and cam-profile" changes), do not take effect after a hitless upgrade.

- FPGA images cannot be upgraded using the hitless upgrade process.

- Hitless upgrade cannot be used to downgrade an image to a version older than the version currently running on the device.

- If there are protocol dependencies between neighboring nodes, it is recommended that you upgrade nodes one at a time.

- After hitless upgrade, the running configuration on the router will be the same as it was before the upgrade. A configuration that is not saved before a hitless upgrade is not removed and the existing startup configuration does not take effect. This behavior is similar to the management module switchover feature.

The Hitless OS upgrade process

A hitless upgrade of Multi-Service IronWare software is performed in the following sequence:

1. Multi-Service IronWare software is installed in flash memory to the primary and secondary image on active and standby management modules and interface modules.

2. Enter the **hitless-reload** command on the active management module.

3. The hitless upgrade process starts on the active management module, which initiates the upgrade process on the standby management module.

4. The standby management module is reset.

5. The active management module is reset and the standby management module becomes the active module.

6. Active console control is lost to the previously active management module as it becomes the standby management module.

7. The active management module initiates the upgrade process on all interface modules.

8. The router is now running the new Multi-Service IronWare software. The management module that was initially configured as the standby management module is now the active management module and the management module that was initially configured as the active management module is now the standby management module. If you want the original management module to be active, you must manually fail-over control to it.

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:

1. **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

2. Device serial number

Getting help or reporting errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Brocade using one of the following options.

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the **Product Documentation** tab, and then click on the link to the Knowledge Portal (KP). Then click on **Cases** > **Create a New Ticket** to report an error. Make sure you specify the document title in the ticket description.

E-mail and telephone access

Go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Additional resources

This section lists additional publications you can reference to find more information about the products supported in this software release.

Title	Contents
Brocade NetIron CES 2000 and NetIron CER 200 Series Hardware Installation Guide	- Product Overview - Installation - Basic Configuration - Hardware Maintenance and Replacement - Fiber optic connectors - Replaceable modules - AC Power supply - Fans - Software Upgrades - Hardware Specifications - Regulatory Statements

Title	Contents
Brocade MLXe and NetIron Family Configuration Guide	Contains all configuration information for the NetIron CES 2000 series of switches.
IronWare MIB Reference	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
Brocade MLXe, NetIron MLX, and NetIron XMR Routers Hardware Installation Guide	- Product Overview - Installation - Redundant Management Module Configuration - Basic Configuration - Hardware Maintenance and Replacement - Air filters - Fiber optic connectors - Replaceable modules - AC Power supply - Fans - Software Upgrades - Hardware Specifications - Regulatory Statements
NetIron MLX and NetIron XMR Diagnostic Reference	This manual describes troubleshooting and diagnostic commands available in the IronWare command line interface (CLI) for NetIron XMR and MLX routing devices.

Open defects in R05.0.00 that were closed in R05.1.00

This section lists defects closed from the previous release. 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.

Defect ID:	DEFECT000272011	Technical Severity:	Medium
Summary:	PIM router may unnecessarily forward multicast traffic to a PIM snoop device which would drop it.		
Workaround:	Avoid using pimsm-snooping on a snoop device located between 2 PIM routers if RP and source are reachable via different paths for one of the PIM routers and the RP is reachable by going through the snoop device.		
Feature:	IPv4-MC Snooping- VLANs	**Function:**	PIM-SM/SSM Snooping
Reported In Release:	NI CES 03.8.00		

Defect ID:	DEFECT000276603	Technical Severity:	High
Summary:	Turning off PPP scramble mode takes effect only after the interface is disable and then enabled		
Workaround:	Disable/enable of the interface after turning off PPP scramble mode		
Feature:	POS	**Function:**	PPP
Reported In Release:	NI 04.0.00		

Defect ID:	DEFECT000279972	Technical Severity:	Medium
Summary:	The 'clear rate-limit counters' command does not reset statistics correctly.		
Workaround:	Issue the 'clear rate-limit counters' command with the interface port number to reset stats correctly.		
Feature:	Rate Limiting - XMR/MLX	**Function:**	Non-ACL based
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000283848	Technical Severity:	Medium
Summary:	When external-lsdb-limit is configured and the 'clear ip ospf all'command is issued, with the max-metric configured for Type-5 External, Summary and Router LSAs, the metric value for NSSA LSAs remain set to the maximum value.		
Workaround:	Enter the 'no redistribute' command, then enter the 'redistribute' command in OSPF after you enter the 'clear ip ospf all' command. Use the following syntax: no redistribute <protocolName> redistribute <protocolName> After reconfiguring the redistribution, NSSA LSAs are regenerated with the proper default metric value.		
Feature:	OSPF	**Function:**	PROTOCOL
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000284237	Technical Severity:	Medium
Summary:	Port security 'deny-mac-address' command is not compatible with software versions 4.0 or earlier.		
Symptom:	After upgrading from 4.0.1a to 4.1.0.0, the 'mac-port-security deny-mac-address' command requires the statement 'vlan' prior to the vlan number. Because of this change, the 'mac-port security' configuration was not applied after reload to 4.1.0.0.		
Feature:	L2 Protocol	**Function:**	PMS
Probability:	Medium		
Reported In Release:	NI 04.1.00	**Service Request ID:**	243673

Defect ID:	DEFECT000285233	Technical Severity:	Medium
Summary:	Output from the 'show module' command reports G1 SFM status as powered-off after a switchover, if the system is configured in turbo mode		
Feature:	System - XMR/MLX	Function:	SFM
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000286068	Technical Severity:	Medium
Summary:	Output from the 'show mpls rsvp session' command says that the detour is down although it is up on transit after failures happen on ingress and merge point routers.		
Symptom:	Occurs when there are two failures, one at the ingress and other at the merge point router. The PLR detour session at transit router will remain down		
Feature:	RSVP-TE	Function:	One-to-one FRR
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000286272	Technical Severity:	Medium
Summary:	When G1 cards are rejected due to Turbo mode, the card down reason given might be incorrect.		
Feature:	System - XMR/MLX	Function:	PERFORMANCE
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000288070	Technical Severity:	Medium
Summary:	Output from the show mpls lsp detail command shows LSP status is down due to 'PathErr: Bad initial subobject' after failures happen on ingress and transit routers.		
Symptom:	This is a double FRR failure case. The first failure occurs at ingress router and the second one occurs at the transit router. The PATH message for the second detour is rejected by the downstream node because the top hop in ERO is not the local address of the receiving router		
Feature:	RSVP-TE	Function:	Facility FRR
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000289261	Technical Severity:	Medium
Summary:	RP Candidate cannot encode more than 64 group prefixes in the advertisement to the BSR		
Symptom:	This limitation was introduced in software because a large number of group-prefixes can lead to buffer corruption. Applies to both IPv4 and IPv6.		
Feature:	IPv4-MC PIM-SM Routing	Function:	PROTOCOL
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000296967	Technical Severity:	High
Summary:	Temporary loss of multicast traffic if an active MP is physically removed from device		
Workaround:	Manually switchover the active MP using the "switch" command before removing it from the device		
Feature:	IPv4-MC PIM-SM Routing	Function:	Switchover
Reported In Release:	NI 05.0.00		

Open defects in R05.1.00

This section lists open defects in Multi-Service IronWare R05.1.00. 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.

Defect ID:	DEFECT000297243	Technical Severity:	High
Summary:	If multicast traffic is mirrored from one 8x10GE packet processor to the other, 2 copies of each		

packet are received.	
Feature: System - XMR/MLX	**Function:** Mirroring
Reported In Release: NI 05.0.00	**Probability:** High

Defect ID: DEFECT000299547	**Technical Severity:** High
Summary: Under certain conditions, multiple reloads of a PB switch might cause downstream PBB MAC entries to be incorrectly programmed.	
Symptom: Data packets might drop due to mis-programming of MAC entries in PB and PBB after reloads.	
Workaround: Enter the command "clear mac HHHH.HHHH.HHHH" for the affected entries.	
Feature: CES 802.1ah	**Function:** Forwarding
Reported In Release: NI 05.1.00	**Probability:** Medium

Defect ID: DEFECT000304391	**Technical Severity:** High
Summary: When MD5 authentication is configured on an interface used by a bypass LSP, the backup RSVP session riding over the bypass LSP does not come up after FRR local repair.	
Workaround: Do not configure RSVP authentication on ingress and egress interfaces used by bypass LSP.	
Feature: RSVP-TE	**Function:** Facility FRR
Reported In Release: NI 05.1.00	**Probability:** High

Defect ID: DEFECT000305951	**Technical Severity:** High
Summary: Packets will be dropped by an egress CER router if it is the merge point for a FRR facility backup.	
Workaround: The CES and CER should not be used as an egress router for FRR facility backup; instead use one-to-one FRR.	
Feature: CES MPLS	**Function:** IPoMPLS
Reported In Release: NI 05.1.00	**Probability:** Low

Defect ID: DEFECT000309023	**Technical Severity:** High
Summary: In a broadcast network consisting of more than 2 MPLS routers, PATH messages might be sent to the wrong hop not present in the ERO object.	
Symptom: LSP's will not come up.	
Workaround: Avoid having multiple MPLS enabled routers in a single IP subnet.	
Feature: RSVP-TE	**Function:** One-to-one FRR
Reported In Release: NI 05.1.00	**Probability:** Low

Defect ID: DEFECT000317888	**Technical Severity:** High
Summary: ISIS on POS modules with HDLC encapsulation does not interoperate with certain 3rd party devices.	
Symptom: Everything works as expected with PPP encapsulation. HDLC works as expected with Brocade XMRs.	
Workaround: Use PPP encapsulation.	
Feature: IS-IS	**Function:** PROTOCOL
Reported In Release: NI 04.0.01	**Probability:** High

Defect ID: DEFECT000317918	**Technical Severity:** High
Summary: ISIS neighbors flap under a stressed MPLS scaled environment with ISIS shortcuts enabled.	
Workaround: Increase the ISIS SPF timers.	
Feature: IS-IS	**Function:** PROTOCOL
Reported In Release: NI 04.0.01	**Probability:** High

Defect ID: DEFECT000318197	**Technical Severity:** High
Summary: Some external LSAs may not be flooded by XMR when advertised by certain 3rd party test	

equipment.	
Workaround:	Ensure that the XMR is elected as the DR.

Feature: OSPF		Function: PROTOCOL	
Service Request ID: 250871			
Reported In Release: NI 05.0.00		Probability: Low	

Defect ID: DEFECT000318235		Technical Severity: High	
Summary: An LSA with a higher metric can prevent the installation of a LSA with a lower metric and a broadcast address LS ID.			
Symptom: When adding a static route on one router, a route for the same network might disappear from another router.			
Workaround: Use the "clear ip ospf debug update" command to trigger a SPF recalculation.			
Feature: OSPF		Function: Redistribution	
Service Request ID: 260272			
Reported In Release: NI 05.0.00		Probability: Low	

Defect ID: DEFECT000318580		Technical Severity: High	
Summary: In a 2-level MCT, after an MP switchover, an innocuous message indicating presence of a loop might appear.			
Symptom: No functional impact.			
Feature: MCT		Function: Port Loop Detection	
Reported In Release: NI 05.1.00		Probability: Low	

Defect ID: DEFECT000319335		Technical Severity: High	
Summary: VRRP MAC ages out on the ICL while receiving hello packets.			
Workaround: Use VRRP-E instead of VRRP for MCT applications.			
Feature: MCT		Function: MLX_VRRPE	
Reported In Release: NI 05.1.00		Probability: Medium	

Defect ID: DEFECT000319453		Technical Severity: High	
Summary: Using the "cp" command to copy a file that is the same size as the free flash space, the management module may experience an unexpected reset.			
Workaround: Ensure that the available flash space is larger than the file being copied.			
Feature: System - XMR/MLX		Function: Boot/Monitor/OS	
Reported In Release: NI 05.1.00		Probability: Low	

Defect ID: DEFECT000319471		Technical Severity: High	
Summary: VRRP-E Virtual MAC learned on the Inter-Chassis Link (ICL) is displayed by the show command as CL on the CER and CR on the MLX.			
Symptom: No functional impact.			
Feature: MCT		Function: MLX_VRRPE	
Reported In Release: NI 05.1.00		Probability: Low	

Defect ID: DEFECT000276825		Technical Severity: Medium	
Summary: Port mirroring configuration on the primary port of a LAG is removed after the LAG is undeployed.			
Workaround: Prior to undeploying a LAG, remove the mirror-port configuration and then reapply it after the LAG is deployed.			
Feature: CES Mirroring		Function: Port Based	
Reported In Release: NI 04.1.00		Probability: Low	

Defect ID: DEFECT000276835		Technical Severity: Medium	

Summary:	When rate-limiting is configured on a LAG, "show rate-limit counters" displays incorrect values.	
Workaround:	Use the "show interface" command.	
Feature: Rate Limiting - XMR/MLX	Function: Non-ACL based	
Reported In Release: NI 04.1.00	Probability: Medium	

Defect ID: DEFECT000277058	Technical Severity: Medium
Summary: Output from the 'show rmon statistics' command shows a larger value for some of the counters after a hitless OS upgrade.	
Workaround: Manually execute 'clear rmon statistics' after a HLOS upgrade.	
Feature: System - XMR/MLX	Function: Ethernet MAC/PHY
Reported In Release: NI 04.1.00	

Defect ID: DEFECT000281775	Technical Severity: Medium
Summary: When there is a pending ARP request, PBR configuration will take a number of seconds to be applied.	
Symptom: The console may appear to be unresponsive.	
Feature: CES IPv4 Forwarding	Function: PBR
Reported In Release: NI 05.0.00	Probability: Low

Defect ID: DEFECT000289707	Technical Severity: Medium
Summary: After restoring an mrp ring in svlan, some traffic is flooded at master node.	
Symptom: In an svlan domain, certain mac-movement events may cause sustained flooding to happen (for example, disabling STP on a svlan, or re-enabling a port of an MRP ring). No fault is reported by the CLI's "show mac" command - the impact is visible only on user's traffic. Such flooding heals itself when the user's traffic stops for about 15 seconds. Alternatively, the flooding can be eliminated by clearing the mac table.	
Workaround: Issue a "clear mac" on the master node.	
Feature: CES 802.1ad	Function: Flood Domain
Reported In Release: NI 05.0.00	Probability: Medium

Defect ID: DEFECT000290408	Technical Severity: Medium
Summary: "show tm-voq" command counters display zero values when "sh stat br" cmd is executed before "st tm-voq" cmd.	
Workaround: Reissue the "show tm-voq" command.	
Feature: System - XMR/MLX	Function: FPGA-Stats
Reported In Release: NI 05.0.00	Probability: Low

Defect ID: DEFECT000296636	Technical Severity: Medium
Summary: During High CPU conditions, optical monitoring might not take effect when enabled on the SFP port.	
Workaround: Reinsert the SFP.	
Feature: System - XMR/MLX	Function: Ethernet Optics
Reported In Release: NI 05.0.00	Probability: Low

Defect ID: DEFECT000312478	Technical Severity: Medium
Summary: "show tech-support cluster" command might not display details for all the VLANs.	
Symptom: When displaying data for more than 60 VLANs, data for some of the VLANs will be missing.	
Feature: MCT	Function: CLI
Reported In Release: NI 05.1.00	Probability: Medium

Defect ID: DEFECT000317894	Technical Severity: Medium

Summary:	ARP response packet size is 94 bytes in XMR/MLX.	
Symptom:	Certain 3rd party firewalls are known to report such ARP packets as violations.	
Feature: IPv4 Forwarding - XMR/MLX		Function: ARP
Reported In Release: NI 04.1.00		Probability: Low

Defect ID: DEFECT000318512		Technical Severity: Medium
Summary: Link-fault-signaling might cause ports on a 10Gx8 module to flap.		
Workaround: Use UDLD.		
Feature: System - XMR/MLX		Function: Link Fault Signaling
Service Request ID: 261889		
Reported In Release: NI 05.0.00		Probability: Medium

Defect ID: DEFECT000319457		Technical Severity: Medium
Summary: On boot-up an innocuous error message will be displayed for secondary ports of the LAG when tag-type is configured on the LAG.		
Symptom: "Error - Cannot configure secondary trunk port 1/15" will be displayed.		
Feature: CES L2 Forwarding		Function: MAC Manager
Reported In Release: NI 05.1.00		Probability: Low
Defect ID: DEFECT000318696		Technical Severity: High
Summary: Rate-limiting policy applied to a 1G port does not take effect after a reload on a chassis with 2x10G modules.		
Symptom: Packets will not be rate-limited.		
Workaround: Remove and add the rate-limit configuration on the interface after reload.		
Feature: CES Rate Limiting		Function: ACL
Service Request ID: 261419		
Reported In Release: NI 05.0.00		Probability: Medium

Defect ID: DEFECT000314496		Technical Severity: High
Summary: BFD session might not reestablish after flapping multiple LAG ports on CER.		
Symptom: "show bfd neighbor" command displays BFD neighbor State as DOWN. This does not impact routing functionality.		
Workaround: Delete and re-add the BFD configuration on the interface.		
Feature: BFD		Function: PROTOCOL
Reported In Release: NI 05.0.00		Probability: Low

Closed defects in R05.1.00

This section lists defects closed with code in Multi-Service IronWare R05.1.00. 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.

Defect ID: DEFECT000275344		Technical Severity: Medium
Summary: In some rare cases, multiple line cards in a system incorrectly had the same base MAC address.		
Symptom: We have a customer case where we observe same MAC address on multiple line cards on same chassis.		
Feature: CES SYSTEM		Function: MAC
Probability: Low		
Reported In Release: NI 04.1.00		Service Request ID: 235608

Defect ID:	DEFECT000276885	Technical Severity:	Medium
Summary:	In certain situations during an area change NetIron XMR did not advertise the Type4 LSA		
Feature:	OSPF	Function:	PROTOCOL
Probability:	Low		
Reported In Release:	NI 04.0.01	Service Request ID:	238030

Defect ID:	DEFECT000278668	Technical Severity:	High
Summary:	Large number of untagged ports in one line may cause stack overflow and unexpected system reload.		
Symptom:	Could not boot system until reset to default configuration.		
Workaround:	Modify the number of ports under vlan 1.		
Feature:	System - XMR/MLX	Function:	Boot/Monitor/OS
Probability:	High		
Reported In Release:	NI 04.0.00	Service Request ID:	240542

Defect ID:	DEFECT000279561	Technical Severity:	Medium
Summary:	Error message displays when using tftp with an ACL in a running config that has "end" at the end of the command string.		
Symptom:	Error message displayed: "Config buffer: session re-entrance error. Issue free-config-buffer command in this window to recover from the error."		
Feature:	System - XMR/MLX	Function:	Boot/Monitor/OS
Probability:	Medium		
Reported In Release:	NI 04.0.00	Service Request ID:	241117

Defect ID:	DEFECT000287234	Technical Severity:	Medium
Summary:	During the Database Exchange procedure, Event BadLSReq may occur when device is a master in DD.		
Feature:	OSPF	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	239184

Defect ID:	DEFECT000288728	Technical Severity:	Medium
Summary:	In certain situations BGP OID 1.3.6.1.4.1.1991.1.2.11.17.1.1.2 returned an incorrect value.		
Feature:	BGP	Function:	PROTOCOL
Probability:	Low		
Reported In Release:	NI 04.0.00	Service Request ID:	240903

Defect ID:	DEFECT000289087	Technical Severity:	High
Summary:	After ISIS adjacency flap, SPF does not run and Level1 routes are not leaked into Level2.		
Symptom:	When adjacency usage is changed from L12 to L1, the L1 routes learned from that adjacency are not leaked to L2.		
Workaround:	Configure the spf-interval to 0. This enables the SPF to run quickly and digest the changes after adjacency flap. i.e., Dut1(config-isis-router)#spf-interval 0.		
Feature:	IS-IS	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	245915

Defect ID:	DEFECT000290385	Technical Severity:	Medium
Summary:	Port info is truncated on logged Optical Monitoring error		
Feature:	SYSLOG	Function:	PROTOCOL

Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	254040

Defect ID:	DEFECT000296280	Technical Severity:	Medium
Summary:	During a BGP scaling test, when a large number of routes have the same AS-path, it might take a long time to learn the routes.		
Feature:	BGP	Function:	BGPv4
Probability:	Low		
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000296884	Technical Severity:	Medium
Summary:	Format flash card command fails with EXCEPTION 0300 - FATClearDriveParaBlk		
Feature:	System - XMR/MLX	Function:	Flash memory
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	249897

Defect ID:	DEFECT000297866	Technical Severity:	Medium
Summary:	Implementation of RFC 5065 is not complete, so BGP selects confidration ebgp route with bad metric over ibgp route.		
Feature:	BGP	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	247681

Defect ID:	DEFECT000298539	Technical Severity:	Medium
Summary:	In some configurations OSPF E2 routes may be inserted in route table with incorrect metric.		
Symptom:	If a route prefix is redistributed as an external type-2 ospf route from two different ASBR's with two different metrics and then advertized across an ABR to a non-ABR MLX, then the metric selected in the route table on the MLX is always the metric from the first route regardless of whether the second prefix received (for the same route) has a lower metric.		
Feature:	OSPF	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	247424

Defect ID:	DEFECT000298645	Technical Severity:	Medium
Summary:	On systems with specific third-party PSU, diagnostic failed with NI 4.1.00 but passed with NI 4.0.00.		
Symptom:	Customer ran diagnostic under NI 4.1.00 and failed with "error:vendorname_i2c_read:status: checksum failure Power supply 0 register read failed". When the diagnostic was run under NI 4.0.0 for the NI-MLX-MR received there was no issue.		
Feature:	System - XMR/MLX	Function:	Diagnostics
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	241890

Defect ID:	DEFECT000298734	Technical Severity:	High
Summary:	High CPU utilization may result in unexpected reload of interface module.		
Feature:	System - XMR/MLX	Function:	IPC/ITC
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	257885

Defect ID:	DEFECT000298812	Technical Severity:	Medium
Summary:	exp option in qos command does not show when in mif configuration		

Feature:	CES QOS		Function:	Encode/Decode Policy
Probability:	High			
Reported In Release:	NI 04.1.00		Service Request ID:	248308

Defect ID:	DEFECT000298837		Technical Severity:	Medium
Summary:	In a scaled up environment, the management module may reload in an MPLS task when the system runs out of memory.			
Symptom:	This occurs only in an extremely rare test configuration.			
Feature:	MPLS Control Plane		Function:	Memory Management
Probability:	Low			
Reported In Release:	NI 03.8.00			

Defect ID:	DEFECT000299484		Technical Severity:	Medium
Summary:	vlan-cpu-protection will cause CPU to generate duplicate packets when more than 2031 vlans are created.			
Symptom:	NA			
Workaround:	Remove cpu protection on the vlan as workaround			
Feature:	L2 Forwarding - XMR/MLX		Function:	Forwarding
Probability:	Medium			
Reported In Release:	NI 04.0.00		Service Request ID:	249307

Defect ID:	DEFECT000299950		Technical Severity:	Medium
Summary:	IPv6 prefix information was being sent twice in RA message.			
Feature:	IPV6		Function:	RTM
Probability:	High			
Reported In Release:	NI 04.1.00		Service Request ID:	249721

Defect ID:	DEFECT000300206		Technical Severity:	Medium
Summary:	In certain situations when a downstream router was rebooted IS-IS routes on the XMR flapped for a period of time			
Feature:	IS-IS		Function:	PROTOCOL
Probability:	Medium			
Reported In Release:	NI 04.1.00		Service Request ID:	248590

Defect ID:	DEFECT000300327		Technical Severity:	Medium
Summary:	No spanning tree after removing vlan from vlan group			
Feature:	L2 Protocol		Function:	Single Spanning Tree
Probability:	Medium			
Reported In Release:	NI 04.1.00		Service Request ID:	248810

Defect ID:	DEFECT000300628		Technical Severity:	High
Summary:	LAG creation within ve on system with large arp table may cause time-sensitive protocol state transition.			
Symptom:	When adding a LAG containing ports which are in a ve, then vrrp protocol packets on a separate interface may fail to get transmitted/received for a few seconds. This results in a flap.			
Workaround:	Adding the LAG in a non-ve first and then tagging it into the vlan/ve will not result in the protocol flaps.			
Feature:	IPv4 Forwarding - XMR/MLX		Function:	ARP
Probability:	Medium			
Reported In Release:	NI 04.1.00		Service Request ID:	245854

Defect ID:	DEFECT000300752	Technical Severity:	Medium
Summary:	Incorrect TM flow mapping is seen on an egress port if qos scheduler is applied on that port.		
Symptom:	Packet loss on one of the LAG ports due to incorrect TM flow mapping to the ingress port.		
Feature:	System - XMR/MLX	Function:	FID/Queue
Probability:	High		
Reported In Release:	NI 04.0.01	Service Request ID:	250047

Defect ID:	DEFECT000300993	Technical Severity:	Medium
Summary:	Failed to remove the Rate-limit policy from interface if the average bit rate has some specific values and average bit rate gets adjusted		
Feature:	CES RL	Function:	ACL Based
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	249904

Defect ID:	DEFECT000301041	Technical Severity:	High
Summary:	Issuing the show log command on the VSRP Master may cause a VSRP flap from Master-Confirm back to Backup		
Feature:	VSRP	Function:	VSRP Master
Probability:	Low		
Reported In Release:	NI 03.9.00	Service Request ID:	250566

Defect ID:	DEFECT000301305	Technical Severity:	Medium
Summary:	MPLS VPLS : With VPLS Load Balancing and module removal or insertion "show mac vpls " command response is affected by a sync issue between MP and LP.		
Symptom:	Response to the "show mac vpls " command is slow.		
Workaround:	Perform "clear mac vpls x" command for the vpls instance involved.		
Feature:	VPLS - XMR/MLX	Function:	Control Plane
Probability:	Low		
Reported In Release:	NI 04.0.00		

Defect ID:	DEFECT000301544	Technical Severity:	Medium
Summary:	FDP packets are prioritized to queue 7 and flooding can cause critical controls packets to be delayed		
Feature:	FDP-CDP	Function:	PROTOCOL
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000301552	Technical Severity:	Medium
Summary:	In rare cases, memory Parity Error may occur after reload/Cold Start, causing loss of connectivity.		
Workaround:	Change system bootup initialization sequence and calibrate memory controller setting.		
Feature:	CES SYSTEM	Function:	Resource Manager
Probability:	High		
Reported In Release:	NI 04.1.00		

Defect ID:	DEFECT000301845	Technical Severity:	Medium
Summary:	Removed cosmetic NetIronCES/CER bootup message: "Chassis and Module type mismatch check enabled"		
Feature:	CES SYSTEM	Function:	Event Manager
Probability:	Low		
Reported In Release:	NI CES 03.9.00	Service Request ID:	250334

Defect ID:	DEFECT000301979	Technical Severity:	Medium

Summary:	DC power supplies p/n 32050 and 32035 displayed as AC in the 'show chassis' output.		
Feature: System - XMR/MLX		Function: POWER SUPPLY	
Probability: High			
Reported In Release: NI 03.7.00		Service Request ID: 251905	

Defect ID: DEFECT000302069		Technical Severity: Medium	
Summary: In certain configurations the CES virtual modules go down due to Heartbeat Loss.			
Feature: CES SYSTEM		Function: IPC/ITC	
Probability: Medium			
Reported In Release: NI 04.1.00		Service Request ID: 250989	

Defect ID: DEFECT000302153		Technical Severity: Medium	
Summary: Show chassis doesn't provide power usage info on most of installed LPs			
Feature: System - XMR/MLX		Function: POWER SUPPLY	
Probability: Medium			
Reported In Release: NI 04.0.01		Service Request ID: 248973	

Defect ID: DEFECT000302230		Technical Severity: Medium	
Summary: show vlan <vlan-id> stats output not displaying line separator with mix of 4x10 and 8x10 modules			
Feature: Extended Counter		Function: L2VLAN	
Reported In Release: NI 05.0.00		Service Request ID: 252580	

Defect ID: DEFECT000302250		Technical Severity: High	
Summary: LSP flaps when going from hot-standby-sec to primary with select-path configuration			
Feature: MPLS Control Plane		Function: LSP Manager	
Reported In Release: NI 05.0.00		Service Request ID: 252581	

Defect ID: DEFECT000302261		Technical Severity: Medium	
Summary: syslog/SNMP displays LSP's RSVP session name instead of given LSP name.			
Feature: RSVP-TE		Function: CLI	
Probability: High			
Reported In Release: NI 05.0.00		Service Request ID: 252582	

Defect ID: DEFECT000302263		Technical Severity: High	
Summary: With Fast port movement within L2VLAN and VPLS-VLAN with the same VLAN-ID,L2 DA cam is not cleared			
Feature: L2 Forwarding - XMR/MLX		Function: Forwarding	
Probability: High			
Reported In Release: NI 05.0.00		Service Request ID: 252583	

Defect ID: DEFECT000302356		Technical Severity: High	
Summary: 1G link may come "UP" even when only RX is connected and TX is not connected.			
Feature: CES SYSTEM		Function: I2C	
Probability: High			
Reported In Release: NI 05.0.00		Service Request ID: 251917	

Defect ID: DEFECT000302380		Technical Severity: Medium	
Summary: ip receive access-list does not work for ip address 32.x.x.x and higher.			
Symptom: With CES connected point-to-point with an MLX. MLX can telnet to CES; however, CES cannot telnet to MLX.			

Feature:	CES ACL	Function:	IPv4
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	251054

Defect ID:	DEFECT000303014	Technical Severity:	Medium
Summary:	IPv6 OSPFv3 orphan routes remain on an interface that is just configured with OSPFv3 IPsecurity when all OSPFv3 neighbors are immediately cleared and brought down.		
Symptom:	No OSPFv3 neighbor relationships exist but OSPFv3 routes remain in the IPv6 routing table.		
Workaround:	On XMR 4.0.00f, "clear ipv6 route" or "clear ipv6 ospf force-spf". On NI 5.0.00, "clear ipv6 ospf all".		
Feature:	OSPFv3	Function:	Clear Commands
Probability:	High		
Reported In Release:	NI 04.0.00	Service Request ID:	253167

Defect ID:	DEFECT000303051	Technical Severity:	High
Summary:	LDP neighbors might flap as a result of high CPU utilization condition on the interface module CPU.		
Symptom:	With this condition, LDP neighbors might flap occasionally.		
Feature:	LDP	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.0.01	Service Request ID:	250945

Defect ID:	DEFECT000303052	Technical Severity:	Medium
Summary:	SFLOW sampling on VPLS/VLL end points might cause duplication of the sampled packets being transmitted.		
Symptom:	This occured when running the RFC2544 test, which was failing on the CER if the sflow was enabled on VPLS/VLL end ports or on the Uplink port.		
Feature:	CES SFLOW	Function:	VLL
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	247950

Defect ID:	DEFECT000303293	Technical Severity:	High
Summary:	Sflow is enabled with non-VRF's and no MPLS configuration.		
Symptom:	In rare situations, the interface module may unexpectedly reload.		
Feature:	Sflow - XMR/MLX	Function:	General
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	253285

Defect ID:	DEFECT000303300	Technical Severity:	Medium
Summary:	Upon receipt of dying-gasp/critical events, the links flap continuously.		
Symptom:	When a dying-gasp and critical events are sent on the link-oam enabled link, the NetIron CES/CER/XMR switches are constantly flapping the links.		
Feature:	802.3ah	Function:	PROTOCOL
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	250406

Defect ID:	DEFECT000303345	Technical Severity:	Medium
Summary:	Interface Module may be shut down due to incorrectly read overheat conditions.		
Symptom:	An incorrect read of 247.500C was attributed to a healthy module.		
Feature:	System - XMR/MLX	Function:	Temp sensor

Probability:	Low		
Reported In Release:	NI 04.0.00	Service Request ID:	249781

Defect ID:	DEFECT000303511	Technical Severity:	High
Summary:	Known unicast frames received on even numbered newly added LAG ports are flooded as if they were unknown unicast frames.		
Symptom:	VLAN-cpu-protection configured on four XMR-32's used as Layer2 switches between 16 third party routers. Those routers are each connected to all four XMR-32's through one- and two-port dynamic LAGs. After expanding multiple existing one-port LAGs to two-port LAGs on all the XMRs, multiple primary LAG ports were sending large numbers of frames, yet the third party server saw only 20 packets per second incoming.		
Workaround:	Clear MACs. Disable vlan-cpu-protection.		
Feature:	LAG - XMR/MLX	Function:	Dynamic
Probability:	High		
Reported In Release:	NI 04.0.00	Service Request ID:	252187

Defect ID:	DEFECT000303637	Technical Severity:	Critical
Summary:	When a non-8x10G module on a running system is replaced by an 8x10G module, traffic from any other pre-existing 8x10G modules to the replaced 8x10G line module may not function properly. This issue is also seen with 48T line modules.		
Feature:	System - XMR/MLX	Function:	FID/Queue
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	253305

Defect ID:	DEFECT000303765	Technical Severity:	Medium
Summary:	ifHCInOctets counters are not updated correctly		
Feature:	SNMP Management	Function:	System Management Mib
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	253685

Defect ID:	DEFECT000303990	Technical Severity:	Critical
Summary:	In rare situations, depending on the sequence of BGP updates, the router may reload unexpectedly.		
Workaround:	n/a		
Feature:	BGP	Function:	BGPv4
Probability:	Low		
Reported In Release:	NI 05.0.00	Service Request ID:	253823

Defect ID:	DEFECT000304140	Technical Severity:	High
Summary:	File from unexpected reset does not save all valid data structures		
Feature:	System - XMR/MLX	Function:	Boot/Monitor/OS
Probability:	Low		
Reported In Release:	NI 05.0.00		

Defect ID:	DEFECT000304211	Technical Severity:	Medium
Summary:	NI 5.0 LP diags failed during CAM check		
Feature:	System - XMR/MLX	Function:	Diagnostics
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	253794

Defect ID:	DEFECT000304260	Technical Severity:	Medium
Summary:	BGP state change trap should be generated only when backward transition is from ESTABLISHED state.		
Symptom:	MIB trap was sent from BGP state other than ESTABLISHED.		
Feature:	SNMP Management	Function:	Trap/Notification
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	251162

Defect ID:	DEFECT000304447	Technical Severity:	Medium
Summary:	Display issue after #sho controller NAME e32/4 command for slot 32 only.		
Symptom:	Error message displayed: Error:cu_show_port_stat: mplp_show_send_request_to_lp() failed (1).		
Feature:	CLI Infrastructure	Function:	Parser Engine
Probability:	High		
Reported In Release:	NI 04.0.01	Service Request ID:	253950

Defect ID:	DEFECT000304704	Technical Severity:	Medium
Summary:	OIDs fdryVllEndPointOutHCOctets and fdryVllEndPointInHCOctets retrun valu 0.		
Feature:	SNMP Management	Function:	MPLS Mib
Reported In Release:	NI 04.1.00	Service Request ID:	254004

Defect ID:	DEFECT000305373	Technical Severity:	Medium
Summary:	Traffic Manager queues may not be mapped correctly for new module swapped with different module type.		
Symptom:	When module did not come up, error message displayed: "failed to come up "Due to mismatch."		
Feature:	System - XMR/MLX	Function:	FID/Queue
Probability:	Medium		
Reported In Release:	NI 04.0.01	Service Request ID:	254597

Defect ID:	DEFECT000305574	Technical Severity:	Medium
Summary:	TACACS+ configuration values for retransmit, timeout and dead-time are overwritten when authorizing with command lines requiring > 1472 TACPLUS+ authorization packet length.		
Symptom:	In the display of a running config, the TACACS values are inflated.		
Workaround:	Split long command lines into multiple lines when entering at CLI.		
Feature:	AAA	Function:	TACACS+ Authorization
Probability:	Medium		
Reported In Release:	NI 04.0.00	Service Request ID:	251351

Defect ID:	DEFECT000306094	Technical Severity:	High
Summary:	In a scaled up environment with a large number of PIM cache fluctuations, multicast task might not release management module buffers, which can result in IPC failures.		
Symptom:	In a network running PIM-SM with ~4500 S,G groups and ~50 neighbors, the PIM cache fluctuated rapidly and the large number of simultaneous changes resulted in 'out of buffer' conditions on the management module.		
Feature:	IPv4-MC PIM-SM Routing	Function:	SCALABILITY
Probability:	Low		
Reported In Release:	NI 04.0.01	Service Request ID:	249142

Defect ID:	DEFECT000306257	Technical Severity:	Medium
Summary:	In certain rare situations or configurations IS-IS routes were not getting updated in the Route Table Manager (RTM).		
Symptom:	Some ISIS routes might not show up in the route table.		

Feature:	IS-IS	Function:	ISISv4
Probability:	Low		
Reported In Release:	NI 04.0.00	Service Request ID:	255632

Defect ID:	DEFECT000306283	Technical Severity:	Critical
Summary:	Unexpected management module reload occurred while issuing the command 'show statistics brief lag' from a Telnet session.		
Symptom:	Unexpected management module reload.		
Feature:	LAG - XMR/MLX	Function:	Dynamic
Probability:	Medium		
Reported In Release:	NI 04.0.01	Service Request ID:	255300

Defect ID:	DEFECT000306383	Technical Severity:	Medium
Summary:	LACP messages received on ports not configured with LACP might get flooded to other ports in the VLAN.		
Symptom:	Third party server was configured for LACP, but not the ports on the MLX side. When the LACP packets were received from the server, they were flooded to the second third party server, which brought its LAG down.		
Feature:	VPLS - XMR/MLX	Function:	Data Plane
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	254813

Defect ID:	DEFECT000306898	Technical Severity:	Medium
Summary:	After Management failover, syslog messages might not contain the hostname.		
Feature:	SYSLOG	Function:	CLI
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	255816

Defect ID:	DEFECT000306928	Technical Severity:	Medium
Summary:	Transit router fails to generate (S,G,RPT) Prune leading to periodic high CPU.		
Feature:	IPv4-MC PIM-SM Routing	Function:	PROTOCOL
Probability:	Low		
Reported In Release:	NI 04.1.00	Service Request ID:	255462

Defect ID:	DEFECT000306946	Technical Severity:	High
Summary:	Management module might reload unexpectedly during hotswap of an SFM module.		
Feature:	System - XMR/MLX	Function:	SFM
Probability:	Low		
Reported In Release:	NI 05.0.00	Service Request ID:	255540

Defect ID:	DEFECT000306963	Technical Severity:	Medium
Summary:	First ping with packet size of 1473 or greater fails if the ARP for the destination is aged out or not present.		
Workaround:	Configuring static arp or making arp aging to be 0 (so that ARP entry does not age out).		
Feature:	IPv4	Function:	Stack
Probability:	Medium		
Reported In Release:	NI 04.0.00	Service Request ID:	219688

Defect ID:	DEFECT000307158	Technical Severity:	Medium
Summary:	A router forwarded the first multicast packet back out on the port on which it was received.		
Symptom:	Customer saw the 1st packet from the mulitcast source on the originating interface. If the (S,G)		

times out the 1st packet from the source is also sent to the originating port. Only seen for the 1st packet additional packets are not sent to the originating port.	
Workaround: None known	
Feature: IPv4-MC PIM-SM Routing	Function: PROTOCOL
Probability: High	
Reported In Release: NI 04.0.01	Service Request ID: 255595

Defect ID: DEFECT000307490	Technical Severity: Medium
Summary: Removing comma after the hostname in syslog.	
Symptom: Since numerous server names are created based on the initial hostname, the server names are all created with the comma interspersed in the name.	
Feature: SYSLOG	Function: PROTOCOL
Probability: Low	
Reported In Release: NI 05.0.00	Service Request ID: 253953

Defect ID: DEFECT000307633	Technical Severity: Medium
Summary: After upgrade to NI 5.0.00, slower BGP convergence noted when receiving multiple full Internet feeds.	
Symptom: Slower convergence compared to NI 4.1.00 version.	
Feature: BGP	Function: PROTOCOL
Probability: High	
Reported In Release: NI 05.0.00	Service Request ID: 253890

Defect ID: DEFECT000307671	Technical Severity: Medium
Summary: Executing "reset mac-dev all" for a 1Gx20-SFP 1GbE-100FX module might result in an unexpected reload of the interface module.	
Symptom: Error message displayed: Soft Check (Timeout) ppc440_loop_udelay(pc).	
Feature: System - XMR/MLX	Function: Diagnostics
Probability: Low	
Reported In Release: NI 03.7.00	Service Request ID: 254599

Defect ID: DEFECT000307897	Technical Severity: High
Summary: When a properly functioning fan is reinserted, it is not correctly recognized.	
Symptom: "Show chassis" lists fan as "invalid."	
Feature: System - XMR/MLX	Function: Fan
Probability: High	
Reported In Release: NI 05.0.00	Service Request ID: 256289

Defect ID: DEFECT000308167	Technical Severity: Medium
Summary: Inconsistent behavior when applying IP address under the ip vrrp	
Symptom: Inconsistent behavior when applying IP address under the ip vrrp vrid 63, it incorrectly sees some IP address as 'broadcasts' while it accepts lower ip addresses fine.	
Workaround: Take lower IP addresses in the subnet.	
Feature: VRRP - XMR/MLX	Function: Forwarding
Probability: High	
Reported In Release: NI 05.0.00	Service Request ID: 254149

Defect ID: DEFECT000308528	Technical Severity: Medium
Summary: Improve Syslog message to identify the rear fans of a 16 slot chassis more accurately , instead of FANTRAY2	
Feature: System - XMR/MLX	Function: MP/LP I2C bus

Reported In Release:	NI 04.1.00	Service Request ID:	256833

Defect ID:	DEFECT000308566	Technical Severity:	Medium
Summary:	Upgrade creates 2 entries for UDLD disable in results for "show snmp server" command.		
Symptom:	Erroneous entry: "no snmp-server enable traps udld" "no snmp-server enable traps udld."		
Feature:	SNMP Management	Function:	CLI
Probability:	Medium		
Reported In Release:	NI 04.1.00	Service Request ID:	255994

Defect ID:	DEFECT000308571	Technical Severity:	Medium
Summary:	BFD packets with unknown non zero value in your discriminator field is not dropped by the router		
Feature:	BFD	Function:	PROTOCOL
Reported In Release:	NI 05.0.00	Service Request ID:	255226

Defect ID:	DEFECT000308578	Technical Severity:	Medium
Summary:	When the tunnel interface is brought down due to recursive reroute or unreachable tunnel destination, the tunnel interface cannot be disable (administratively brought down).		
Feature:	IP Tunnel - XMR/MLX	Function:	GRE
Reported In Release:	NI 05.0.00	Service Request ID:	255502

Defect ID:	DEFECT000309007	Technical Severity:	Medium
Summary:	Port polling debugging process has been enhanced with further activity checks.		
Symptom:	In rare cases after hosts reload, the link on a particular module will not recover using Brocade/Foundry SR optics.		
Feature:	System - XMR/MLX	Function:	Ethernet MAC/PHY
Probability:	Low		
Reported In Release:	NI 05.0.00	Service Request ID:	252639

Defect ID:	DEFECT000309757	Technical Severity:	Medium
Summary:	Interface module may reload unexpectedly when debug ip pim add-del-oif is enabled.		
Symptom:	This situation occurs only when debugging is enabled.		
Feature:	IPv4-MC PIM-SM Routing	Function:	Debug
Probability:	Low		
Reported In Release:	NI 04.1.00		

Defect ID:	DEFECT000310620	Technical Severity:	Medium
Summary:	After management module switchover some system-max values may revert to default.		
Symptom:	This has been observed after a management module switchover on a 32-slot chassis, only when not all of the routes were populated in the routing table.		
Feature:	System - XMR/MLX	Function:	Boot/Monitor/OS
Probability:	Low		
Reported In Release:	NI 04.0.01	Service Request ID:	257705

Defect ID:	DEFECT000310660	Technical Severity:	Medium
Summary:	Dynamically chosen IPv6 ACL sequence numbers can overlap with previously specified, statically configured sequence numbers.		
Symptom:	ACL lines are listed in the running and startup configs in an order other than the one in which they were configured.		
Workaround:	Either manually configure sequence numbers on all lines in a given ACL, or don't manually configure sequence numbers on any lines in a given ACL.		

Feature: ACL - XMR/MLX		Function: IPv6 ACL
Probability: High		
Reported In Release: NI 05.0.00		Service Request ID: 257985

Defect ID: DEFECT000310783		Technical Severity: Medium
Summary: After losing connectivity to TACACS+ server and then regaining connectivity, the console prompt would be missing the '>' or '#' and would not take any input		
Workaround: no enable aaa console <enter> on console enable aaa console		
Feature: AAA		Function: CLI
Probability: Medium		
Reported In Release: NI 04.0.00		Service Request ID: 251353

Defect ID: DEFECT000310942		Technical Severity: Medium
Summary: BFD-MIB returns invalid/incorrect		
Feature: SNMP Management		Function: Routing Mib
Reported In Release: NI 05.0.00		Service Request ID: 257262

Defect ID: DEFECT000311238		Technical Severity: Medium
Summary: In some cases (with ECMP routes with paths pointing to IPoMPLS interface and regular interface), the PRAM entry for the IPoMPLS route may point to the CPU.		
Symptom: Traffic dropped on some route destinations.		
Workaround: Putting a "permit ip any any" ACL at ingress resolves the issue. All the packets are still software forwarded.		
Feature: MPLS Forwarding - XMR/MLX		Function: IPoMPLS
Probability: Medium		
Reported In Release: NI 04.0.01		Service Request ID: 257205

Defect ID: DEFECT000311246		Technical Severity: Medium
Summary: Connection Admission Control should be performed on receiving PATH message.		
Symptom: In customer case we have seen 2 issues: 1. Tunnel is UP at ingress but down on transit due to CAC failure 2. Re-opt fails at ingress due to CAC on transit but since we do not send PATH_Error toward upstream, Ingress keeps on attempting to re-optimize		
Feature: MPLS Control Plane		Function: Resource Manager
Probability: High		
Reported In Release: NI 04.0.01		Service Request ID: 258052

Defect ID: DEFECT000311521		Technical Severity: Medium
Summary: 4 ECMP vrf paths not load balancing correctly		
Workaround: disable/enable non-working port slowly can fix the problem		
Feature: MPLS Forwarding - XMR/MLX		Function: L3VPN 2547
Reported In Release: NI 05.0.00		Service Request ID: 257196

Defect ID: DEFECT000311690		Technical Severity: High
Summary: Memory Leak in MPLS hop pool		
Symptom: Failed to create the MPLS path hop, due to lack of memory,.		
Feature: MPLS Control Plane		Function: Memory Management
Probability: High		
Reported In Release: NI 04.1.00		Service Request ID: 258342

Defect ID:	DEFECT000311806	Technical Severity:	Medium
Summary:	gre one-armed traffic may get dropped on ingress		
Symptom:	Customer traffic ingressing on GRE tunnel was dropped by MLX if next-hop was on same ve as GRE tunnel endpoint.		
Feature:	IP Tunnel - XMR/MLX	Function:	GRE
Reported In Release:	NI 04.1.00	Service Request ID:	256803

Defect ID:	DEFECT000312914	Technical Severity:	Medium
Summary:	snmp server ipv4 acl leaves server vulnerable to ipv6 probes and vice versa		
Symptom:	In a dual stack ipv4 and ipv6 environment when snmp ipv4 acls are applied against a community string, an ipv6 query cannot be blocked to the snmp server using that string. Similarly an ipv4 query cannot be blocked to the snmp server using the ipv6 community string. This is a vulnerability.		
Feature:	SNMP Management	Function:	Engine
Reported In Release:	NI 05.0.00	Service Request ID:	257184

Defect ID:	DEFECT000313476	Technical Severity:	Medium
Summary:	System stops logging denied traffic and on lp console we see message Can not log ACL denied traffic[No L4 session can be created]		
Feature:	ACL - XMR/MLX	Function:	Deny Logging
Probability:	Medium		
Reported In Release:	NI 04.0.00	Service Request ID:	258080

Defect ID:	DEFECT000313947	Technical Severity:	Medium
Summary:	Incorrect FID mask for a newly inserted module, when FID is reallocated from OLD module to New module.		
Feature:	System - XMR/MLX	Function:	FID
Reported In Release:	NI 04.0.00	Service Request ID:	259240

Defect ID:	DEFECT000313978	Technical Severity:	Medium
Summary:	Device does not flood igmp report if ve for the vlan is disabled.		
Feature:	IPv4-MC IGMP	Function:	IGMP - multi-version support
Reported In Release:	NI 04.0.00	Service Request ID:	258077

Defect ID:	DEFECT000314410	Technical Severity:	Medium
Summary:	CES updates CAM entries every 1 second due to loop terminating condition not hit for label propagate TTL updates.		
Workaround:	Turn off the label propagate ttl and reboot.		
Feature:	CES MPLS	Function:	IPoMPLS
Reported In Release:	NI 05.0.00	Service Request ID:	252778

Defect ID:	DEFECT000314438	Technical Severity:	High
Summary:	In rare circumstances, the interface module may be reset unexpectedly as a result of TM errors.		
Symptom:	In these rare circumstances, the software attempts to recover the line module from TM errors, and in some cases that results in the software power cycling the line module.		
Feature:	System - XMR/MLX	Function:	SFM
Probability:	Low		
Reported In Release:	NI 04.0.00	Service Request ID:	247759

Defect ID:	DEFECT000315089	Technical Severity:	Medium
Summary:	Remove ACL logging command for IP Receive ACLs on CES and CER.		
Feature:	CES ACL	Function:	ACL Deny Logging
Reported In Release:	NI 05.0.00	Service Request ID:	259608

Defect ID:	DEFECT000315094	Technical Severity:	Medium
Summary:	Dynamic lag port's VLAN 1 configuration was erased after reload.		
Feature:	CES L2 Forwarding	Function:	Vlan Transaltion
Reported In Release:	NI 05.0.00	Service Request ID:	259605

Defect ID:	DEFECT000315272	Technical Severity:	Medium
Summary:	Output of show ip route longer shows route from one vrf in another vrf.		
Feature:	IPv4	Function:	show commands
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	259479

Defect ID:	DEFECT000315334	Technical Severity:	Medium
Summary:	In some cases stale detour RSVP sessions may remain on a router.		
Symptom:	In some cases we might have stale detour RSVP sessions on a router. This causes new detour sessions to not come UP.		
Feature:	MPLS Control Plane	Function:	DC-MPLS Stack
Probability:	High		
Reported In Release:	NI 05.0.00	Service Request ID:	256920

Defect ID:	DEFECT000315576	Technical Severity:	Medium
Summary:	Provide backword compatibility support for L2 registration process for RX release 2.5.00x and prior.		
Feature:	IPv4-MC PIM-SM Routing	Function:	PROTOCOL
Probability:	Medium		
Reported In Release:	NI 04.0.01	Service Request ID:	249362

Defect ID:	DEFECT000316621	Technical Severity:	Medium
Summary:	Member VLANs are not added to topology groups at boot if the master VLAN's untagged ports have RSTP disabled on the interface.		
Symptom:	The regression symptom was found by our customer for their evaluation. The problem they found is, Bug#88396 is still seen on both 4.1 and 5.0 code train. Trackweb Bug ID: 88396 Synopsis: Member VLANs are not added to topology groups at boot if the master VLAN's untagged ports have RSTP disabled on the interface.		
Workaround:	The following config can be read from the startup config with no problems: ====================== vlan 2 untagged ethe 1/1 tagged ethe 1/2 to 1/3 rstp priority 10000 rstp ethernet 1/1 disable rstp ethernet 1/2 admin-pt2pt-mac rstp ethernet 1/3 admin-pt2pt-mac ! vlan 100 tagged ethe 1/2 to 1/3		

```
                !
                vlan 101
                 tagged ethe 1/2 to 1/3
                !
                vlan 102
                 tagged ethe 1/2 to 1/3
                 !
                topology-group 1
                 master-vlan 2
                 member-vlan 100 to 102
                =======================
```

Feature: Topology Group	Function: VLAN Members
Probability: Medium	
Reported In Release: NI 04.1.00	Service Request ID: 259857

Defect ID: DEFECT000316779	Technical Severity: Medium
Summary: MLX :- Issue when configuring ACLs using INM on a MLX 5.0.00b	
Symptom: When applying an ACL with a port mapping it removes the mapping when deploying	
Workaround: Use CLI to configure ACL	
Feature: ACL - XMR/MLX	Function: IPv4 ACL
Reported In Release: NI 05.0.00	Service Request ID: 00259253

Defect ID: DEFECT000317068	Technical Severity: Medium
Summary: The service type table for a regular VLAN were deleted by VPLS.	
Workaround: There are 3 workarounds for this: 1. Simply remove the port form the L2 VLAN that had this issue and then add the port back to it again. or 2. wait for 20 munites before deleting the VPLS instance after the port was remvoed from the VPLS local endpoint. 3. Don't remove the port from the VPLS local endpoint and just delete the instance itself.	
Feature: VPLS - XMR/MLX	Function: Control Plane
Probability: Medium	
Reported In Release: NI 05.0.00	Service Request ID: 261093

Defect ID: DEFECT000317390	Technical Severity: Medium
Summary: Management module reloaded with EXCEPTION 1100, after "show task" in OS mode.	
Feature: Console	Function: DISPLAY
Probability: High	
Reported In Release: NI 05.0.00	Service Request ID: 261246

Defect ID: DEFECT000317607	Technical Severity: Medium
Summary: VSRP ip address is not reachable via VPLS local swithing	
Symptom: VSRP ip address is not reachable via VPLS local swithing Steps to recreate: RX 1/1 ------------------------ 1/2 MLX (1/3 --1/4) vlan 100 vlan 100 1. According to above topology, on MLX, 1/2 and 1/3 are VPLS end points and are tagged for vlan 100. 1/4 are tagged fro vlan 100, NOT VPLS end point. 1/3 and 1/4 are looped back. MLX has ve 100 with ip 192.168.200.1. Under vlan 100, layer3 VSRP is also configured with ip	

192.168.200.2

2. on RX, 1/1 is tagged for vlan 100 and ve 100 is configured with ip 192.168.200.10

3. Issue ping from RX, VSRP ip is not reachable

Feature:	VPLS - XMR/MLX	Function:	Data Plane
Reported In Release:	NI 05.0.00	Service Request ID:	257532

Defect ID:	DEFECT000317788	Technical Severity:	High
Summary:	Unexpected reload on Management Module after LAG port removal of VLL end-point		
Feature:	LAG - XMR/MLX	Function:	Dynamic
Probability:	High		
Reported In Release:	NI 04.0.00	Service Request ID:	261436

Defect ID:	DEFECT000317847	Technical Severity:	Critical
Summary:	Unexpected reload of the Management module when issuing OSPF commands with MPLS FRR configured.		
Feature:	RSVP-TE	Function:	One-to-one FRR
Reported In Release:	NI 05.0.00	Service Request ID:	261613

Defect ID:	DEFECT000317889	Technical Severity:	Medium
Summary:	Traps generated by BGP session transitions use bogus peer addresses for IPv6 neighbors.		
Feature:	BGP	Function:	BGPv6
Reported In Release:	NI 04.0.01	Service Request ID:	260636

Defect ID:	DEFECT000317906	Technical Severity:	Medium
Summary:	dns_pm_callback causes unexpected dns reset		
Feature:	DNS	Function:	PROTOCOL
Reported In Release:	NI 05.0.00	Service Request ID:	259631

Defect ID:	DEFECT000317953	Technical Severity:	High
Summary:	After some link flaps CSPF mapping unresolved errors were noted with OSPF TE		
Feature:	MPLS Control Plane	Function:	TED
Probability:	Medium		
Reported In Release:	NI 05.0.00	Service Request ID:	261639

Defect ID:	DEFECT000318431	Technical Severity:	Medium
Summary:	replacing SFM with HSFM on 5000c not coming up		
Symptom:	When we replace SFM with HSFM we see that the HSFM does not come up and it reports as powered-off		
Feature:	System - XMR/MLX	Function:	SFM
Reported In Release:	NI 05.0.00	Service Request ID:	261938

Defect ID:	DEFECT000283003	Technical Severity:	Medium
Summary:	Change gig auto negotiation behavior on CES/CER		
Symptom:	Currently, between two gig fiber intefaces, when one side is configured with gig-default auto(default), the other side is gig-default neg-off, links show up at both sides. Default behavior will change to: the side with neg-off configured shows link up and the side with auto configured shows link down.		

In addition: gig-default auto-full is added to switch back to the current behavior (none-default behavior after the code change).	
Feature: CES SYSTEM	**Function:** Auto-negotiation
Probability: Medium	
Reported In Release: NI CES 03.9.00	**Service Request ID:** 242203

Defect ID: DEFECT000307188	**Technical Severity:** Medium
Summary: The "copy-sflow" feature may reflect the incoming packets applied by an ACL back on the incoming port	
Feature: CES SFLOW	**Function:** ACL-based
Probability: Medium	
Reported In Release: NI 05.0.00	**Service Request ID:** 255931