BROCADE

Multi-Service IronWare Software Release 04.1.00b for Brocade NetIron Family

Release Notes v1.1

March 17, 2010

Document History

Document Title	Summary of Changes	Publication Date
Multi-Service IronWare Software Release 04.1.00b for Brocade NetIron Family Release Notes v.1.0	Initial release	March 16, 2010
Multi-Service IronWare Software Release 04.1.00b for Brocade NetIron Family Release Notes v.1.1	Updated show version and show flash outputs for NetIron XMR and NetIron MLX	March 17th, 2010

Contents

About This Patch Release

Patch release 04.1.00b is the first generally available patch following release 04.1.00. This document includes updated information regarding image file names, open defects, and a new CLI command for setting the IPv6 Default Router Preference value.

Supported Devices for Multi-Service IronWare Release 04.1.00b

This software release applies to the following Brocade products:

- 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 CER 2048FX
- NetIron CER 2024C
- NetIron CER 2024F
- NetIron CER 2048C
- NetIron CER 2048CX
- NetIron CER 2048F
- NetIron CER 2048FX

Summary of Enhancements for Multi-Service IronWare Release 04.1.00

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 release 04.1.00 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

Protocol features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 Multi-VRF	Beginning in this release, IPv6 has been enhanced to support Multi-VRFs. Each VRF can run OSPFv3, PIM-SM and static routes independently of the other VRF.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
OSPF conditional default route origination with route-map	An enhancement has been made to originate default routes into an OSPF routing domain using route maps. See "Configure default route origination" in the NetIron Configuration Guide.	New	New	New	New	New	New	New
Route map new match attribute "protocol" for OSPF redistribution and default route	A new match option has been added to the route-map command that supports protocol route types. See "Matching based on ISIS protocol type", "Matching based on BGP static network", and "Matching based on RIP protocol type" in the NetIron Configuration Guide.	New	New	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 learned route preference over static-network route	When the device uses the BGP4 algorithm to select a route to send to the IP route table, one of the parameters the algorithm uses is the local preference. Local preference is an attribute that indicates a degree of preference for a route relative to other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message. See "Changing the default local preference" in the NetIron Configuration Guide	Supported	Supported	Not Supported	New	New	New	New
BGP Route Maps continue statement	A continuation clause in a route-map directs program flow to skip over route-map instances to another, user-specified instance. If a matched instance contains a continue clause, the system looks for the instance that is identified in the continue clause. See "Route-map continue clauses for BGP routes" in the NetIron Configuration Guide	Supported	Supported	Not Supported	New	New	New	New
BGP four-byte autonomous system numbers ASNs for IPv4 and VRFs	BGP Four-byte ASNs for IPv4 and VRFs are supported in this release. See "Four-byte Autonomous System Numbers"in the NetIron Configuration Guide.	Supported	Supported	Not Supported	New	New	New	New
Show ip ospf interface command with interface filters	Beginning with release, the show ip ospf interface command is enhanced to include an interface filter type that allows you to display OSPF enabled interfaces based on per port type. See "Displaying OSPF interface information" in the NetIron Configuration Guide.	Supported	Supported	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
The redistribution command has been renamed	The redistribution command has been changed to redistribute. See "Define redistribution filters" in the NetIron Configuration Guide	New	New	New	New	New	New	New

MPLS features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 802.1ah (PBB) ISID mapping into VPLS	The new ISID Mapping to VPLS feature allows the customer service instance to be identified end-to-end across the Ethernet and VPLS networks thus enabling fine-grained service treatment at the MPLS edge. See "ISID mapping to VPLS" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
VPLS load balancing modulo enhancement	Starting in this release, load-balancing of VPLS traffic across MPLS LSPs has been enhanced. See "LSP load balancing for VPLS traffic" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Double tag mapping to VPLS and Local VPLS	Beginning with this release, MPLS VPLS and Local VPLS support dual-tagged endpoints. See "Specifying the endpoint of a VPLS instance" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Double tag mapping to VLL	Beginning with this release, VLLs support dual-tagged endpoints. See "Specifying a VLL endpoint" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
IPv4 snooping over double tag for VPLS	Multicast traffic reduction is supported for dual-tagged VPLS endpoints. See "Multicast traffic reduction per VLAN or VPLS instance" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
VPLS Tagged Mode support	With this release, VPLS tagged mode is supported, thus preserving the customer VLAN tag across the MPLS network. See "VPLS tagged mode"in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Resetting MPLS LDP Neighbors	Beginning with this release, the clear mpls ldp neighbor command allows the user to clear all or specific MPLS LDP neighbor sessions. See "Resetting LDP neighbors" in the NetIron Configuration Guide	New	New	Not Supported	New	Not Supported	Not Supported	New
Resetting RSVP-TE LSPs	Beginning with this release, the clear mpls lsp <lsp-name> command allows the user to reset RSVP-TE LSPs.. See "Resetting LSPs" in the NetIron Configuration Guide.	New	New	Not Supported	New	Not Supported	Not Supported	New
Enhanced MPLS LDP FED display	The show mpls ldp fec output has been enhanced to display all Forwarding Equivalence Classes (FECs) that are more specific than with just an IP address.	New	New	Not Supported	New	Not Supported	Not Supported	New
FRR detour LSPs	This release supports detour LSPs, which provide one-to-one protection for RSVP-TE LSPs. See "MPLS fast reroute using one-to-one backup" in the NetIron Configuration Guide.	Supported	Supported	Not Supported	New	Not Supported	Not Supported	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Deprecate show mpls rsvp traffic command	Beginning with this release, the show mpls rsvp traffic command has been deprecated. To display the ingress LSP statistics, use the show mpls statistics lsp command. See "Displaying LSP accounting statistics" in the NetIron Configuration Guide.	Supported	Supported	Not Supported	Supported	Not Supported	Not Supported	Supported

Layer 2 features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Up to 500 Named Layer 2 ACLs	There can be up to 500 named L2 ACLs. See"Types of Layer-2 ACLs" in the NetIron Configuration Guide	New	New	New	New	New	New	New
Layer 2 ACL-Based Rate Limiting	Layer 2 ACL-based rate limiting enables devices to limit the rate of incoming traffic in hardware, without CPU intervention. Rate limiting in hardware enables the device to manage bandwidth at line-rate speed. See"Layer 2 ACL-based rate limiting" in the NetIron Configuration Guide	New	New	New	New	New	New	New
Packet Queuing enhancement	The ip drop-arp-pending-packets command has been added to allow pending ARP requests to be dropped. See "IP packet queuing"in the NetIron Configuration Guide.	Not Supported	Not Supported	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Disabling Gratuitous ARPs for Local Proxy ARP	In this release, you can control whether to reply to a gratuitous ARP request under the Local Proxy ARP configuration. See“Disabling gratuitous ARP requests for Local Proxy ARP”in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New
UDLD on tagged ports	You can configure ports to send out UDLD control packets that are tagged with a specific VLAN ID as tagged UDLD control packets. See “UDLD for tagged ports”in the NetIron Configuration Guide.	New	New	New	New	New	New	New
BGP address-family based neighbor and summary display enhancement	The address-family based neighbor and summary information display will filter out BGP peering that is not configured for this address-family. If BGP peer is configured, but not negotiated with neighbor after BGP peer is in establish state, then a (NoNeg) will be added to end of line for that BGP peering display. See “Displaying summary BGP4 information”and “Displaying summary neighbor information”in the NetIron Series Configuration Guide.	Supported	Supported	New	New	New	New	New
IEEE 802.3ah OAM for L2	In this release, The IEEE 802.3ah Ethernet in the First Mile (EFM) OAM is supported. See “IEEE 802.3ah EFM-OAM” In the NetIron Configuration Guide.	New	New	Not Supported	Supported	Supported	Supported	Supported
IEEE 802.1ag for VPLS Endpoints	Support for IEEE 802.1ag VPLS endpoint was added for the NetIron CES and NetIron CER. See “Ethernet OAM capabilities” in the NetIron Configuration Guide.	Supported	Supported	Not Supported	New	Not Supported	Not Supported	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 VSRP	VSRP has been enhanced to support Layer 3. You can use this enhancement to support redundancy and sub-second failover for Layer 3 topologies. See "Virtual Switch Redundancy Protocol (VSRP)" in the NetIron Configuration Guide.	Supported	Supported	New	New	New	New	New

Forwarding features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
GRE and IPv6 tunnels debug enhancements	Improvements to the IP tunnel debug commands for added granularity. See the NetIron XMR and NetIron MLX Diagnostic Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
VRRP-E enhancement for server virtualization	VRRP-E has been enhanced to optionally allow a VRRP-E backup router to directly forward data and bypass the VRRP-E master router. See "VRRP-E Extension for Server Virtualization" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Scaling of VRRP-E & VRRP instances to 2000	With this release, VRRP-E and VRRP can support a configuration of 2000 instances. See "Overview of VRRP" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
VRF-Lite for IPv6 Multicast	Beginning with this release, IPv6 multicast is now supported over VRFs. See sections "Enabling IPv6 PIM-SM for a specified VRF" through section "Clearing the IPv6 MLD group membership table cache" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
PIM SSM Range ACL	Beginning with this release, you can configure multiple PIM SSM group ranges using an ACL. See section, "Configuring multiple SSM group ranges" and "Displaying information for PIM SSM range ACL" in the NetIron Configuration Guide.	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
OSPFv3 Virtual-Link Enhancement: Dynamic Tunnel Calculation	If there are multiple OSPFv3 Virtual Links between two Area Border Routers using different transit areas, the router has been enhanced to automatically select a global IPv6 address for each transit area and to advertise this address into the transit area. See section "Modify virtual link parameters" in the NetIron Configuration Guide.	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
PIM & MLD Snooping for IPv6 (L2)	This release is enhanced to support IPv6 PIM and MLD snooping for NetIron XMR and NetIron MLX. See section, "IPv6 Multicast Listener Discovery (MLD) Snooping" in the NetIron Configuration Guide.	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 VRF Forwarding *See note below*	Beginning with this release, you can set the CAM mode to dynamic IP CAM mode, and IPv6 CAM mode. IPv6 VPN CAM now supports ECMP load sharing. The show ipv6 cache command and clear ipv6 cache is supported for VRF. See sections "Configuring FDR for IPv6 routes", "Configuring FDR for IPv4 and IPv6 VPN routes", "Enabling support for network-based ECMP load sharing for IPv6", "Displaying IPv6 cache information", "Clearing the IPv6 cache" and "Displaying IPv6 VPN CAM information" in the in the NetIron Configuration Guide.	Supported	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Note: Using a pre-4.1 configuration file which includes IPv6 addresses for non-default VRFs can generate a "VRF(xxx) does not have the IPv6 address family activated" error when upgrading to the 04.1.00 IronWare release. If you encounter this error, you can address it using one of the following two methods:

If an IPv6 address was applied to the VRF interface in error:

1. Remove any interface-level IPv6 configurations from the associated interface(s). Global IPv6 addresses are removed during the boot process, but link-local addresses (both automatically generated and manually configured) remain until they are manually removed.
2. Save the changes to the startup config file.

To make the IPv6 address functional on the VRF interface:

1. From VRF configuration mode, use the address-family ipv6 command to activate the IPv6 family for the selected VRF.
2. From interface configuration mode, re-enter the IPv6 address for the interface.

System features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 CAM Profiles for IPv6 VRF	This release is enhanced to support new CAM profiles for IPv6 VRF. This release provides: Two new CAM profiles (multi-service-3 and multi-service-4) for IPv6 VPN. See sections "CAM partition profiles" and "Displaying CAM Partition for IPv6 VPN" in the NetIron Configuration Guide.	New	New	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
CAM Partitions and enhancements	This release provides: New IPv6 VPN CAM partition. Changes to the IPv6 ACL CAM format. IFL CAM is changed from zero to eight. New IFL CAM format is introduced. The show cam-partition usage output displays the information for CAM usage by the IPv6 VPN. See sections "Output from show CAM partition usage command", "Displaying IPv6 VPN CAM information", "Show cam v6acl", "Show IFL CAM ISID partition", "Configuring CAM partition size","Displaying Network Processor statistics" and "Configuring system max values" in the NetIron Configuration Guide	New	New	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
CLI Changes for Global Commands: ip mtu, spanning-tree, flow-control, ipv6 mtu	Beginning with this release, several global CLI commands have been moved to a different position in the CLI hierarchy. The affected commands are: flow-control, ip mtu, ipv6 mtu, and spanning-tree. See sections "Disabling or re-enabling flow control", "Globally changing the IP MTU", "Changing the IPv6 MTU", "Enabling or disabling STP globally" in the NetIron Configuration Guide.	New	New	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Rename Foundry Networks to Brocade in General output	Beginning with this release, Foundry Networks, Inc. has been changed to Brocade Communications Systems, Inc. in the show version output. See section, Displaying version information in the Brocade NetIron XMR Series Hardware Installation Guide, Brocade NetIron MLX Series Hardware Installation Guide, and Brocade NetIron CES 2000 and NetIron CER 2000 Hardware Installation Guide.	New	New	New	New	New	New	New
I2C Messages Reporting in Syslog	Beginning with this release, when an I2C failure occurs on a management module, a set of static and dynamic syslog messages are generated in the output of the show logging command. A syslog message is also sent to the SNMP log server. See section, Monitoring the status of an I2C failure on a management module in the Brocade NetIron XMR Series Hardware Installation Guide and the Brocade NetIron MLX Series Hardware Installation Guide.	New	New	New	New	New	New	New
Avoid System Reload/Reset During Image Downloading	Beginning with this release, when executing the switchover, reload, and reboot-standby commands, if a software image download is in progress, a warning message is displayed on the console asking the user to confirm the transaction. See sections “Manually switching over to the standby management module” and “Rebooting the active and standby management modules”in the NetIron Configuration Guide.	New	New	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Enhanced Switch Fabric Monitoring	Log messages have been added to indicate changes in the Up/Down status of Switch Fabric Module (SFM) links, and to alert the user when a Fabric Element is inaccessible. Traffic Manager egress error monitoring has also been enhanced. See "Syslog messages system" in the NetIron Configuration Guide.	New	New	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Enhanced show telnet and show who commands	The show telnet and show who commands have been enhanced to display the privilege level of a user. See "Telnet and SSH connections"in the Brocade NetIron Diagnostic Reference.	New	New	New	New	New	New	New
ACL Accounting per Clause	Statistics for inbound and outbound packets denied by ACLs are gathered for individual ACL clauses. See section "ACL accounting on the NetIron CER 2000 and NetIron CES 2000" in the NetIron Configuration Guide.	Not Supported	Not Supported	New	New	New	New	New
Port MAC Security Ehancement	The disable command has been added to the MAC Port Security feature. This command can be applied to a specific interface or global configuration. The interface level take precedence over the global configuration. See "Configuring the MAC port security feature" in the NetIron Configuration Guide.	New	New	New	New	New	New	New

Management Features

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
Support for IEEE 802.1ag MIB	This release adds partial support for IEEE 802.1ag MIB. See the "IEEE8021-CFM-MIB" section in the IronWare MIB Reference The domain-name and ma-name CLI commands have been enhanced to support the IEEE 802.1ag MIB. See "Creating a Maintenance Domain" and "Setting Maintenance Domain parameters" in the NetIron Configuration Guide	New	New	New	New	New	New	New
Updated MIB objects for CAM partitions	The snCamProfile and snCamUsageL3Type SNMP MIB objects to support the new CAM partitions and profiles available in this release. See "CAM Profile" and "CAM Usage for Layer 3 Traffic" in the IronWare MIB Reference	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Increased Syslog Buffer Size	The syslog buffer size has been increased and now the user can configure the system to store up to 5000 entries. See "Changing the number of entries for the local buffer" in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New
Layer 2 Traceroute	This release adds support for trace-l2 which traces the traffic path to a specified device in a VLAN. Also, it can be used to probe all reachable paths to all devices in a VLAN. See "Trace-l2 protocol"in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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
L2VPN MIB enhancements	The following enhancements to the SNMP MIB have been implemented to support L2VPN: The fdryVllEndPointInHCOctets and fdryVllEndPointOutHCOctets objects have been added to the fdryVllEndPoint table to support octet counters for the NetIron CES and NetIron CER.	Not Supported	Not Supported	New	New	New	New	New
	The fdryVplsEndPoint2Table has been enhanced to support dual tags for L2VPN VPLS. This table supports both inner VlAN ID and ISID value for a given endpoint VLAN ID. The vplsConfigServiceType has been updated to support VPLS tagged Mode. See "VLL End Point Table", "VPLS End Point 2 Table" and "vplsConfigTable" in the IronWare MIB Reference	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
New traps	The following traps are introduced in the NetIron XMR and NetIron MLX: snTrapTMEgressDataError which is generated when the system detects egress data errors on Traffic Manager. snTrapSFMAccessError, which is generated when the system fails to access an SFM. See "Traps for Traffic Manager" in the IronWare MIB Reference	New	New	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
LAG ID Preservation	Beginning with release 04.1.00, LAG IDs are now preserved across system reboot. The system automatically generates LAG IDs and the user has the option of configuring LAG IDs. See "Configuration of a LAG" in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New

Enhancement	Description	NetIron XMR Series	NetIron MLX 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 MIB object for LAG ID	The snLinkAggregationGroupTable has been made obsolete beginning with release 04.1.00 for the NetIron XMR, MLX, CES, and CER. It has been replaced by the fdryLinkAggregationGroupTable. Sec "Link Aggregation Group (LAG) Table" in the IronWare MIB Reference	Supported	Supported	New	New	New	New	New
Support for AS 4 byte numbers	The following MIB files have been enhanced to support the BGP AS 4 byte number: snBgp4GenLocalAs4 bgpPeerRemoteAS bgp4PathAttrASPathSegment bgp4PathAttrAggregatorAS See "BGP4 General Variables" and "RFC 4273: Definitions of Managed Objects for BGP-4" in the IronWare MIB Reference	Supported	Supported	New	New	New	New	New
AES Encryption for SSH v2, Secure Copy (SCP), and Secure HTTP (HTTPS)	SSH v2, SCP, and HTTPS now supports a very strong AES encryption algorithm in the following modes: aes256-cbc, aes192-cbc, and aes128-cbc. See "Enabling specific access methods" in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New
Enhancements to SCP to support image downloads	Beginning with this release, enhancements to SCP to support image downloads were added. See "Secure Copy feature for NetIron CES and NetIron CER"in the NetIron Configuration Guide	Supported	Supported	New	New	New	New	New

Summary of Enhancements for the NetIron XMR and NetIron MLX in Release 04.0.01

Enhancement	Description
Protocol features	
BGP AS4 Confederation Error Checking	This section describes the handling of the confederation path segments in the AS4_PATH attribute, and also specifies the error handling for the new attributes AS4_PATH and AS4_AGGREGATOR that are specified in RFC 4893 to support four-byte ASN.
Show ip ospf interface command with interface filters	Beginning with release 04.0.01, the show ip ospf interface command is enhanced to include an interface filter type that allows you to display OSPF enabled interfaces based on per port type.
MPLS features	
Resetting RSVP-TE LSPs	Beginning with release 4.0.01 clear mpls lsp <lsp-name> command allow the user to reset RSVP-TE LSPs.
Resetting MPLS LDP Neighbors	Beginning with release 4.0.01, the clear mpls ldp neighbor command allows the user to clear all or specific MPLS LDP neighbor sessions
IEEE 802.1ag over VLL	Beginning with release 4.0.01, IEEE 802.1ag feature has been enhanced to work with VLL endpoints.
IS-IS Shortcuts	Beginning with release 4.0.01, IS-IS Shortcuts enable an MPLS RSVP-TE path to serve as a shortcut through the network to a destination based on the path's cost (metric). The shortcut can optionally be announced to other routers within the IS-IS routing domain.
VPLS Broadcast or Multicast or Unknown-Unicast Packet Limiting	This feature limits number of Broadcast or Multicast or Unknown-Unicast packets across all VPLS instances that are flooded by a line module CPU.
Multicast features	
Optimization of Multicast Replication and Platform Independence	Beginning with release 04.0.01, Multicast Outgoing Interface List Optimization tracks all the OIF lists in the system. Each multicast route entry maintains a list of outgoing interfaces (OIF List) to which an incoming multicast data packet matching the route is replicated.
Forwarding features	
Policy-Based Routing over a GRE Tunnel	Beginning with release 4.0.01, a GRE Tunnel can be used as the Next Hop used in a PBR policy
ICMP Error Message Rate Increase	Beginning with release 04.0.01, you can configure the maximum ICMP error message rate on all interface modules to 5000 error messages per second.
Deprecate IEEE 802.1p keyword priority as part of IPv6 ACL	Beginning with release 04.0.01, the IPv6 ACL filter containing the keyword, priority-mapping has been deprecated. On upgrading to the new image, IPv6 ACL filters containing this keyword will be rejected.
LAG ID Preservation	Beginning with release 04.0.01, LAG IDs are now preserved across system reboot. The system automatically generates LAG IDs and the user has the option of configuring LAG IDs.
DHCPv6	Beginning with release 04.0.01, DHCPv6 has been enhanced to support the DHCPv6 IPv6 relay agent.
System feature	
Show Media Enhancements	Beginning with release 04.0.01, you can display media information for SFP and XFP on all transceivers per port.
Configurable CAM Size for IPv4 and IPv6 Multicast entries	Beginning with release 04.0.01, system-max commands are added to allow you to configure the CAM size for IPv4 and an IPv6 multicast entries.

Enhancement	Description
Enhanced Syslog for Module State Changes	Beginning with release 04.0.01, the NetIron system now logs the status change of a module when the module becomes Up or Ready or Down due to a software change. The show log command allows you to view the logged messages.
System Low Memory Prevention and Reporting	Beginning with release 04.0.01, when system-max value values are configured, the NetIron system will now check for available system resources. System-max values are checked at configuration time, and at bootup time. Dynamic memory allocation failures are also monitored on the Management Module and Interface Module.
System Max Configurable Memory Checking	Beginning with release 04.0.01, when system-max value values are configured, the NetIron system will now check for available system resource, and if there is not enough available resources, the configuration will be rejected.
Logging of Dynamic Memory Allocation Failures	Beginning with release 04.0.01, the system will monitor the amount of available memory and in case of low memory or memory allocation failures will generate warnings.
Increased Syslog Buffer Size	Beginning with release 04.0.01, the syslog buffer size has been increased and now the user can configure can configure the system to store up to 5000 entries.
High Speed Fan Support for MLX-16	When installing 1Gx48-T modules, the NetIron MLX-16 chassis requires upgrading of the rear fan modules to NI-X-16-FAN-EXH-A modules.
10GE Port Local Fault Counters and Logging	Beginning with release 04.0.01, the user can display and clear local fault counters with the CLI. Syslog messages are now generated when a port goes down due to a local fault.
Option to delete old image first upon image download if MP Flash full	Beginning with release 04.0.01, the system can automatically delete and old image first before upgrading if it needs to make space on the flash.
Security features	
New Encoding Scheme for storing passwords, authentication keys, and community strings on the system	Beginning with release 04.0.01, the encoding scheme for storing various attributes has been changed to a more secure mechanism and it affects the following attributes: BGP: neighbor MD5 authentication key OSPF: authentication-key OSPF: MD5 authentication key OSPF: area virtual link authentication key OSPF: area virtual link MD5 authentication key OSPFv3: ipv6 ospf authentication, area authentication, and area virtual authentication ISIS: authentication key MPLS TE: rsvrp authentication MPLS LDP: session key RADIUS: global key RADIUS: per host key TACACS+: global key TACACS+: per host key SNMP: read and write community string SNMP: trap host community string Configurations with encryption code 2 are not compatible with earlier releases.
Enhanced security for IPv6 management access	Beginning with release 04.0.01, the system supports the use of IPv6 ACLs to restrict management access.

Enhancement	Description
Management feature	
Support for GRE Tunnels in SNMP MIB	Beginning with release 04.0.01, the following MIB tables have been updated to support GRE tunnels: tunnelIfTable tunnelInetConfigTable ifTable ifXTable snIfIndexLookupTable snIntefaceLookupTable
New MIB object for LAG ID	Beginning with release 04.0.01, the snLinkAggregationGroupId object has been enhanced to support the ID that has been assigned to a LAG.
Remote Network Monitoring Management Information Base MIB updated to RFC 2819	Beginning with release 04.0.01, Remote Network Monitoring has been updated to RFC 2819.
New notification for module state changes	Beginning with release 04.0.01, the snTrapModuleStatusChange notification is generated when a module operational state changes.
Show media MIB information table.	Beginning with release 04.0.01, a new MIB table has been added lists media device information (SFP, XFP, and copper physical port) Ethernet ports.
New MIB objects for board serial number, board part number, and chassis part number.	The SNMP object snAgentConfigModuleSerialNumber in the snAgentConfigModuleTable has been deprecated in this release. To replace this object, snAgentBrdSerialNumber and snAgentBrdPartNumber were added to the snAgentBrdTable. Also, snAgentConfigModuleSerialNumber was added to the snAgentConfigModuleTable
Enhancements to SCP to support copying code and FPGA images	Beginning with release 04.0.01, Added enhancements to SCP to support images downloads.

Summary of Enhancements for the NetIron XMR and NetIron MLX in Release 04.0.00

Enhancement	Description
Hardware Features	
Optical Monitoring Capable Optics	1000Base-LHB SFP optic, SMF, LC connector. Optic Monitoring Capable For ranges up to 150 Km Part # E1MG-LHB-OM
	100Base-BXU SFP optic SMF, a single strand of SMF fiber, LC connector. Optic Monitoring Capable Transmits at 1310nm and receives at 1550nm This optic should only be connected to an E1MG-BXD at the far end. Part # E1MG-BXU-OM
	100Base-BXD SFP optic SMF, a single strand of SMF fiber, LC connector. Optic Monitoring Capable Transmits at 1550nm and receives at 1310nm This optic should only be connected to an E1MG-BXU at the far end. Part # E1MG-BXD-OM

Enhancement	Description
	100Base-BXU SFP optic SMF, LC connector. Transmits at 1310nm and receives at 1550nm. Optic Monitoring Capable This optic should only be connected to an E1MG-100BXD at the far end. Part # E1MG-100BXU-OM
	100Base-BXD SFP optic SMF, LC connector. Transmits at 1550nm and receives at 1310nm. Optic Monitoring Capable This optic should only be connected to an E1MG-100BXU at the far end. Part # E1MG-100BXD-OM
New Optic	New 10G optic for FDDI-grade fiber. For ranges up to 200 meters MM fiber, compatible with 10GBASE-LRM optics Part # 10G-XFP-1310-MMF
NI-MLX-1Gx48-T Modules	Beginning with this release, the MLX supports the NI-MLX-1Gx48-T modules.
Protocol Features	
Requiring the First AS to be the Neighbor's AS	Beginning with release 04.0.00, you can specify that the first AS listed in the AS_SEQUENCE field of an AS path update message from EBGP neighbors must be the AS of the neighbor that sent the update. The feature can be applied globally for the router or for a specific neighbor or peer group
IS-IS SPF Scaling	Beginning with release 04.0.00, IS-IS scalability has been enhanced. The new disable-incremental-spf-opt command has been added to prevent certain network changes from causing SPF recalculation.
BGP Four-byte AS numbers	Beginning with release 04.0.00, BGP four-byte AS numbers are supported.
RTM Scalability Enhancement	Beginning with release 04.0.00, next-hop entries in RTM are consolidated to increase efficiency of resource usage. The show ip route nexthop command and show ip route command display this change.
Route Map Continue Clause	Beginning with release 04.0.00, a continue clause in a route map can cause program flow to skip to a specific entry. This enhancement applies only to route maps used within BGP.
Limiting Advertisement of a Static BGP Network	Beginning with release 04.0.00, you can control the advertisement of a static BGP network to BGP neighbors that are configured as Service Edge Routers.
MPLS Features	
BGP-based auto-discovery for VPLS	BGP-based auto-discovery for VPLS (also called VPLS auto-discovery) eliminates the need for manual configuration of VPLS peers for every VPLS instance configured on the device.
BGP Shortcut Enhancement	Beginning with release 4.0.00, LSP metrics can be used in determining the cost to IGP next hops.
Dual-tags for VLL-local	Beginning with release 04.0.00, the dual-tag support feature lets a port accommodate dual tag VLLs. The dual tag feature enables local VLLs to recognize packets with two tags.
Show Command to Display TE path	Beginning with this release, you can display a traffic engineering path to a IPv4 destination address using a specified set of resource parameters.
Option of FEC Type for Auto-discovered VPLS Peers	By default, Foundry uses FEC 129 to send the VC label binding for auto-discovered VPLS peers. Beginning with Release 04.0.00, an option is available that allows the router to use FEC 128 for auto-discovered VPLS peers.
Enhancements to MPLS path and route display	Beginning with release 04.0.00, the show mpls path and show mpls route outputs have been enhanced to display more information.

Enhancement	Description
Enhancement to an MPLS RSVP debug command	Beginning with release 04.0.00, the debug mpls rsvp packets command supports both directions at an interface and also now supports debugging MPLS RSVP on a POS interface
In support of CSPF, more informative display output for MPLS LDP	Beginning with release 04.0.00, the show mpls ldp fec output has been enhanced to display all Forwarding Equivalence Classes (FECs) that are more specific than with just an IP address.
Multicast Features	
Multicast over GRE Tunnel	Beginning with this release, IPv4 multicast over a point-to-point GRE tunnel is now supported.
IPv4 and IPv6 PIM Anycast RP	This release supports PIM Anycast RP for both IPv4 and IPv6 multicast domains. PIM Anycast RP is a method of providing load balancing and fast convergence to PIM RPs in an IPv4 and IPv6 multicast domain. When the source is activated in a PIM Anycast RP domain, the PIM First Hop (FH) will register the source to the closest PIM RP. The PIM RP follows the same MSDP Anycast RP operation by decapsulating the packet and creating the (s,g) state.
Layer-2 Features	
VSRP Slow Start	VSRP slow start timer feature provides a specified amount of time to elapse between the time the Master is restored and when it takes over from the Backup. This interval allows time for VSRP convergence when the Master is restored.
VLAN Translation Feature Retired	Beginning with release 04.0.00, the VLAN Translation feature which used the vlan-translate-group command has been retired. Its functions are now being supported using the Local VLL and Local VPLS features.
Layer-3 Features	
Statistics for GRE and Manual IPv6 Tunnels	Beginning with release 04.0.00, statistics can be accumulated for GRE and manual IPv6 tunnels in both directions and for multicast and unicast modes.
New minimum GRE keepalive	Beginning with release 04.0.00, the minimum time for a GRE tunnel keepalive is 1 second (was 2 seconds). The default keepalive value remains the same.
Forwarding Features	
Disabling Gratuitous ARP Requests for Local Proxy ARP	Beginning with release 04.0.00, you can control whether to reply to a gratuitous ARP request under the Local Proxy configuration.
Dynamic ARP Inspection (DAI)	Beginning with release 04.0.00, Dynamic ARP Inspection (DAI) is supported. DAI enables a device to intercept and examine all ARP request and response packets in a subnet and discard those packets with invalid IP to MAC address bindings created using DHCP Snooping.
DHCP Option 82 insertion	Beginning with release 04.0.00, DHCP Option 82 insertion is supported. DHCP Option 82 insertion is used to assist DHCP servers in determining the location of the client.
IP Source Guard	Beginning with release 04.0.00, IP Source Guard is supported. IP Source Guard permits traffic from only valid source IP addresses.
System Features	
LFS or RFN Counters for 10G LAN PHY	This feature adds dedicated CLIs to display and clear Remote Fault Notification counters (RFN). This is only applicable to 10GbE interfaces in LAN PHY mode.
Power Supply Monitor and Shutdown	Beginning with release 04.0.00, new commands are introduced to monitor the power supply state, and manually shutdown the power supply.
LP Boot-up Failure Signaling to MP	Beginning with release 04.0.00, a new set of boot-up logging messages for interface modules are introduced.

Enhancement	Description
QoS for NI-MLX-1Gx48-T Modules	Beginning with release 04.0.00, the NetIron configuration allows you configure more ports in the system by changing the QoS priorities from 8 to 4 priorities per port. This enables the NetIron chassis to support 2016 ports using 4 priorities per port.
Security Features	
IPsec for OSPFv3	Beginning with release 4.0.00, IPsec can be applied to an interface, area, or virtual link that is using OSPFv3.
CLI changes to Port Security	The port security command at the global level has been changed to distinguish it from the interface level command. The new global-port-security command is used to enable or disable MAC port security at the global level.
Network Management Features	
AES Encryption for SSH v2, Secure Copy (SCP), and Secure HTTPS (HTTPS)	SSH v2, SCP, and HTTPS now supports a very strong AES encryption algorithm in the following modes: aes256-cbc, aes192-cbc, and aes128-cbc.
6to4 Tunnel MIB Support	SNMP support for 6to4 tunnels is provided by the tunnelIfTable and tunnelInetConfigTable of RFC 4087. Furthermore, the snIfIndexLookupInterfaceId of the snIfIndexLookupTable and the snInterfaceLookupInterfaceId of the snInterfaceLookupTable has been updated to support 6to4 tunnels.
CAM MIB	The snCamUsageSessionType of the snCamUsageSessionTable is updated with values for the IP Source Guard feature. The new values are obtained with an SNMP GET or GET NEXT.
Layer 2 ACL MIB objects	You can define Layer 2 ACLs using SNMP.
Support for AS 4 byte numbers	The following MIB files have been enhanced to support the BGP AS 4 byte number: The snBgp4GenLocalAs object has been added to the IronWare enterprise MIB The bgpPeerRemoteAS object in the bgpPeerTable has been enhanced The bgp4PathAttrASPathSegment and bgp4PathAttrAggregatorAS objects in the bgp4PathAttrTable have been enhanced
Support for dual tags for VLL-local	The “fdryVllEndPointInnerVlanId” object has been added to the fdryVllEndPointTable to support dual tagged frame translations at both ingress and egress ports of a local VLL.
gigabitEthernet (117) or fastEther(62) returned for ifType	Issuing the snmp-server legacy iftype allows ifType to return gigabitEthernet (117) or fastEther(62) for Ethernet interfaces
Increased ifIndex for ports	The number of interface indexes (ifIndex) that can be assigned per port has been enhanced. You can now assign 20, 40, or 64 indexes per module.
New enumeration values for snAgentConfigModuleType	Values for snAgentConfigModuleType object in the SNMP MIB have been changed in Release 04.0.00 for the NetIron XMR and NetIron MLX to resolve enumeration conflicts with other hardware modules in the enterprise MIB. The new snmp-server legacy module-type CLI command has been added to allow snAgentConfigModuleType to return the values used before Release 04.0.00.
New support for RFCs	The following RFCs are now supported: 4022 — Management Information Base for the Transmission Control Protocol (TCP) 4113 — Management Information Base for the User Datagram Protocol (UDP) (NetIron XMR and NetIron MLX only) 4293 — Management Information Base for the Internet Protocol (IP) Each of these RFCs provides one table for both IPv4 and IPv6.

Summary of Enhancements for the NetIron XMR and NetIron MLX in Release 03.9.01

Enhancement	Description
Protocol Features	
BGP address-family based neighbor and summary display enhancement	Beginning with this release, the address-family based neighbor and summary information display will filter out BGP peering that is not configured for this address-family. If BGP peer is configured, but not negotiated with neighbor after BGP peer is in establish state, then a (NoNeg) will be added to end of line for that BGP peering display.
MPLS Features	
MPLS Fast Reroute Bypass LSP	This feature enables multiple RSVP-TE LSPs to have a Fast Reroute backup through a shared bypass LSP. The bypass LSP is a tunnel that implements facility (one-to-many) backup. The benefit is greater network resiliency through bypass LSP's greater scalability and nearly hitless protection.
LSP Ping and Traceroute for FRR Bypass LSPs	Beginning with this release, you can ping or execute a traceroute on a bypass LSP. You can ping or trace the route on the ingress-originated or transit-originated bypass tunnel by specifying the bypass LSP name or the RSVP session ID.
Multicast Features	
RFC 3513 and RFC 4007 Compliance for IPv6 multicast scope-based forwarding	Per RFC 3513, packets with an IPv6 destination multicast address with scope 0 or 3 are not forwarded. Also, scopes 1 and 2 are defined as Node-Local and Link-Local and are not forwarded. Only packets with an IPv6 multicast destination address with scope 4 or higher are forwarded. Per RFC 4007's definition of scope zones, the forwarding of packets received on any interface of a particular scope zone are restricted to that scope zone. Foundry supports 1 zone for each scope, and the default zone for scope 4 and higher consists of all interfaces in the system, so the default zones for scope 4 and higher are the same size.
Layer-2 Features	
Increase in default max-frame size	Beginning with release 03.9.01, the default max-frame size for Ethernet ports has been increased from 1544 to 1548 bytes.
Forwarding Features	
ARP Pending Retry Timer	This feature allows you to configure an ARP Pending Retry Timer that will send out three ARP request packets for a configured period until ARP is resolved to prevent large amounts of ARP requests from flooding the network, during network host scanning activity. This feature also includes an enhancement to the ARP refresh timer so that you are able to enter a timer value between 1 and 500.
Network Management Features	
Additional support for VLL and VPLS SNMP MIB tables	The fdryVllEndPointInHCPkts and fdryVllEndPointOutHCPkts MIB objects in the fdryVllEndPointTable are now supported. Also, the MIB object fdryVplsEndPointOutHCPkts in the fdryVplsEndPointTable is now supported.
ethernetCsmacd(6) returned for ifType	During an SNMP get, ethernetCsmacd(6) will be returned as the value of iftype for Ethernet interfaces, instead of gigabitEthernet (117) and fastEther(62). This is in compliance with RFC 2863.

Enhancement	Description
Consolidation of VPLS and VLL Syslog messages for remote peers	When an event affects multiple VLL and VPLS instances (for example, a VLL endpoint is going down) individual Syslog messages and SNMP notifications are generated for all affected remote VLL and VPLS instances. This process can result in a large number of messages for individual instances in the Syslog. In release 03.9.01, this process has been optimized. Only one Syslog message and SNMP notification will be generated for an event that affects multiple VLL and VPLS instances.

Summary of Enhancements for the NetIron XMR and NetIron MLX in Release 03.9.00

Enhancement	Description
Hardware Features	
New Optic Modules – Optic Monitoring Capable	1000Base-LHA SFP optic, SMF, LC connector. For ranges up to 80 Km Part # E1MG-LHA-OM
	100Base-FX SFP optic, MMF, LC connector. Part # E1MG-100FX-OM
	100Base-FX IR SFP optic, SMF, LC connector. For ranges up to 15 Km Part # E1MG-100FX-IR-OM
	100Base-FX LR SFP optic, SMF, LC connector. For ranges up to 40 Km Part # E1MG-100FX-LR-OM
Protocol Features	
Enhanced Support for IPv4 and IPv6 DNS Queries	With this release, we have enhanced the support for IPv4 and IPv6 DNS Record queries to allow IPv4 and IPv6 DNS record queries to search through IPv4 and IPv6 DNS servers.
IP Static Interface Route Across VRFs	Using this feature, you can configure an IP Static interface route from one VRF through an IP Interface in a different VRF. This allows you to connect from one VRF to a host that is directly connected to a port in a different VRF.
Support for ICMPv6 RFC 4443	With this release, RFC 4443 is fully supported for ICMPv6. RFC 4443 supersedes RFC 2463. In addition, new counters have been added to the output of the show ipv6 traffic command in support of this enhancement.
IS-IS Blackhole avoidance	Beginning with release 03.9.00, a new option has been added to the set-overload-bit command to prevent route blackholing in support of RFC 3277.
OSPF Administrative Distance Control Using Route Maps	Beginning with release 03.9.00, the OSPF Distribute List command has been enhanced to use Route Maps. This allows you to selectively set the OSPF Administrative distance.
BGP Neighbor Local-AS	This feature allows you to configure a router so that it can appear to a neighbor to be a member of an AS different from the AS it really belongs to. This feature is useful when two provider networks merge.
DHCP Relay Enhancement	Beginning with this release, the IP subnet configured on the port which is directly connected to the device sending a BootP or DHCP request, does not have to match the subnet of the IP address given by the DHCP server.

Enhancement	Description
Displaying IPv4 and IPv6 Route Uptime	In this release, the output from the show ip route and show ipv6 route commands has been enhanced to display the uptime of a route in the IPv4 and IPv6 routing tables. The uptime measures the time since the route was first created or last modified.
BGP Processing Optimization for Administratively down peers.	Introduced in this release, this enhancement optimizes route processing of administratively down peers by not pre-calculating a rib-out for these peers.
BGP Debug Enhancement	This release contains enhancements to the debugging capabilities in BGP. These includes enhanced per-neighbor debug statements in BGP and new per-neighbor BGP debug filters.
BGP Outbound Policy Processing Optimization	BGP Outbound Policy Processing Optimization has been implemented in this release that results in improved performance for policy processing. This enhancement applies to peers sharing exactly the same outbound policy.
MPLS Features	
BFD for RSVP-TE LSPs	Support has been provided in this release for using BFD with RSVP-TE LSPs. This feature provides a mechanism to detect data plane failure for MPLS LSPs. Advantages to this feature include faster failure detection and automatic detection of faults on a large number of LSPs without a need for manual interaction.
LDP TImers Per Interface	This feature allows you to set separate LDP Hello Intervals and LDP Hello Hold Times for specified interfaces.
Displaying MPLS LDP UpTime	In the release, the output from the show mpls ldp detail command has been enhanced to display the LDP Session Up Time. The Up Time is the time since the LDP adjacency is established. It is displayed in days, hours, minutes and seconds.
LDP Packet Statistics Display	This feature provides the ability to collect and display LDP packet statistics.
Multicast Features	
Concurrent Operation of Multicast Snooping and Routing (IPv4 only)	Beginning with this release, IPv4 multicast routing and multicast snooping instances can work concurrently on the same router as long as multicast snooping and routing are not enabled on the same VE interface or VLAN.
Support for Prune Wait Timer for PIM DM	This feature allows you to configure a Prune Wait timer that specifies the amount of time a PIM DM router will wait before stopping traffic to neighbor routers that do not want the traffic.
Hardware-based forwarding for (*,G) for IPv4 or IPv6	Forwarding for (*,G) for IPv4 or IPv6 allows you to configure intermediate routers between a PIM RP and PIM First Hop (FH) to be optimized to aggregate multicast flows destined to the same group address. This feature move operation of this capability to hardware which results in improved performance.
Layer-2 Features	
Dynamic LAG support for VSRP	Beginning with this release, VSRP is supported over dynamic LAGs.
Sub-second Timers for IEEE 802.1ag	This release supports sub-second values for IEEE 802.1ag. This enables faster fault detection in the network.
Forwarding Features	
DHCP Snooping	This feature allows a device to filter untrusted DHCP messages, and prevent MiM (Man in the Middle) attacks.
Option to Disable VPLS Local Switching	This feature allows you to disable VPLS local switching behavior on a per VPLS basis using the no vpls-local-switching command.

Enhancement	Description
Dynamically Adding or Deleting Ports from a Currently Deployed LAG	This feature allows you to dynamically add or delete ports (except the primary port) from a currently deployed LAG without having to undeploy it.
System Features	
Pre-allocating Memory for User Sessions	In low memory conditions configuration commands can fail to execute because not enough memory is available to the CLI session. This feature allows you to pre-allocate enough memory for the CLI session to maintain operation regardless of system memory usage. This is accomplished through the introduction of a system-max parameter for the configuration file size which is applicable to both startup-config and running-config. Using this parameter, adequate memory resources can be reserved so that at least one session (console, telnet or SSH) remains functional in low memory conditions.
LFS or RFN Status Display for 10GbE LAN PHY	This feature provides information that an Interface has gone down due to Link Fault Signaling Remote Fault Notification (LFS or RFN). When this fault occurs, a Syslog message is generated to inform you of the event and the event is indicated in the output from the show interface command. This is only applicable to 10GbE interfaces in LAN PHY mode.
Fast LP Power-Down	The lp fast-powerdown command has been introduced to immediately shutdown all interface modules in a chassis after a router reload is issued. This can be used in situations when it is not desirable for line cards to continue forwarding while the management module is reloading.
show interface and show statistics information	This output from the show interface and show statistics commands for an Ethernet port have been enhanced to provide a more detailed and accurate display of utilization statistics. A description of the fields displayed is provided.
Interface Module FPGA Bundled Images	The process for upgrading FPGA images has been simplified to allow you to upgrade FPGA images for all NetIron interface modules at the same time.This has been accomplished by providing a bundled FPGA image that contains all of the FPGA images required for all of the Interface Modules installed on a router. You can use this bundled image to upgrade all the Interface FPGA images on a router using a single command.
APS for IPv4	Beginning with release 03.9.00, POS Modules supports Linear-Bi-directional (1+1) APS for a single router. Linear Bi-directional APS consists of two ports, a Working port and a Protect port. In the case of signal failure or degradation, traffic is switched from the Working port to the Protect port.
Power Budget Checking Upon Boot-up	Upon power-up it has been the normal procedure for the system to make sure that the router remains within it's power budget. If it does not, modules exceeding the power budget are prevented from coming up. With this release, this function has been extended to apply when an Interface module is hot-swapped into a router.
Network Management Features	
AES for SNMP v3	The Advanced Encryption Standard (AES) provides one of the most advanced encryption capabilities available today. This release adds AES for SNMPv3 as specified in RFC 3826.
Support or IETF VPLS-Generic-Draft-01-Mib	This release provides support for the VPLS-Generic-Draft-01-Mib module of draft-ietf-l2vpn-vpls-mib-01.
New Foundry MIBs for VPLS, VLL and local VLL	Enterprise MIB for VPLS, VLL, and local VLL, (the fdryVplsTable, fdryVllEndPointTable, and fdryVplsEndPointTable) have been added which provide additional features over the current IETF MIBs. These tables can be used to configure VPLS and VLL end points, as well as additional VPLS instance properties using SNMP.
Enhanced support for Pseudo Wire MIB	Support for the pwTable and pwEnetTable of the Pseudo Wire MIB now includes support for VPLS, VLL, and local VLL.

Enhancement	Description
Notifications for VPLS, VLL. and local VLL	SNMP notifications have been introduced in this release to support the following: MPLS VPLS MPLS Local VLL MPLS VLL Also, the following enhancements have been made to existing traps: The Pseudo Wire traps have been enhanced to provide notification for VPLS peers, VLL and VLL local services. The linkDown and linkUp under the System Status traps have been enhanced to provide notification for VPLS end points state changes.
New Syslog messages for VPLS, VLL, and local VLL	New Syslog messages have been added for the VPLS and local VLL services. These Syslog messages are generated when the service transitions from an up to a down state and vice versa.
IP MIB	The MIB for IP has been updated to the latest IETF standard: RFC 4293: Management Information Base for the Internet Protocol (IP). This MIB supports both IPv4 and IPv6.

Summaries of Enhancements from Earlier Software Releases

For lists of enhancements made to the software for the NetIron XMR, NetIron MLX or NetIron CES in earlier software releases, please refer to the appropriate version of the *Netiron Configuration Guide.*

Supported Features for the NetIron Family

The following tables describe all of the features supported on the NetIron family of devices. In the following section ("Unsupported Features"), there is a list of features not supported on devices in the NetIron family. Features or options not listed in the tables below or documented in this guide are not supported.

System Level Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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
High Availability	Hitless Software Upgrade Hitless Layer 2 Failover Hitless Layer 3 Failover (BGP and OSPF)	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

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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
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

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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
	Per-clause statistics for inbound and outbound packets denied by ACLs	No	No	Yes	Yes	Yes	Yes	Yes

Layer 2 Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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 802.1d	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	Yes	Yes	Yes	Yes	Yes
IEEE 802.1d	Spanning Tree Protocol (STP) Single Spanning Tree Protocol (SSTP)	Yes	Yes	No	No	No	No	No
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
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	Yes	Yes	Yes	Yes	Yes

Category	Feature description	NetIron XMR Series	NetIron MLX 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) Single Spanning Tree Protocol (SSTP)	Yes	Yes	No	No	No	No	No
IEEE 802.1s	Multiple Spanning Tree Protocol within the default ESI (Ethernet Service Instance).	No	No	Yes	Yes	Yes	Yes	Yes
IEEE 802.1s	Multiple Spanning Tree Protocol	Yes	Yes	No	No	No	No	No
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
Brocade MRP	Brocade Metro Ring Protocol (MRP) Phase 1 and Phase 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PVST or PVST+	Per-VLAN Spanning Tree (PVST) within the default ESI (Ethernet Service Instance).	No	No	Yes	Yes	Yes	Yes	Yes
PVST or PVST+	Per-VLAN Spanning Tree (PVST)	Yes	Yes	No	No	No	No	No

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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 Protocol-Based VLANs VLAN Transparent Hardware Flooding	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VLANs	Super Aggregated VLANs (SAV) VLAN Translation	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

Advanced Layer 2 Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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
Ethernet Service Instance (ESI)	RSTP and STP for C-VLANs, S-VLANs and B-VLANs when using the ESI framework 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	No	No	No	Yes	No	No	Yes
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	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 allows or blocks forwarding of Layer 2 protocol packets under a user-configured ESI.	No	No	No	Yes	No	No	Yes
VLAN Translation		Yes	Yes	No	Yes	No	No	Yes

Layer 3 Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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
IPv4 ACLs	Standard and Extended Inbound and Outbound ACL logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Category	Feature description	NetIron XMR Series	NetIron MLX 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 notifications as per RFC 4273 Multi-protocol BGP Extended Communities Route Refresh Co-operative BGP Route Filtering Graceful Restart Helper	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
	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	Yes	Yes	No	Yes	Yes	Yes	Yes

Category	Feature description	NetIron XMR Series	NetIron MLX 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	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	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	No	No	No	No	No
Multi-VRF	Multi-VRF for IPv4 Unicast (OSPF, BGP, Static)	Yes	Yes	No	Yes	Yes	Yes	Yes
RIP Versions 1 and 2	RIP routes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VRRP and VRRPE	Virtual Router Redundancy Protocol (VRRP) and VRRP Extended (VRRPE)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

QoS Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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	No	No	Yes	Yes	Yes	Yes	Yes

VPN Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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
Topology Groups	A named set of VLANs and VPLS endpoints that share a Layer 2 topology. You can use topology groups with the following 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	Yes	Yes	No	No	No	No	No
Layer 3 VPN	BGP/MPLS VPNs (RFC 2547bis) OSPF Sham Link Support Support for RFC 4382: MPLS-L3VPN Standard MIB Multi-VRF Per-VRF VRRP-E Static Routes Across VRFs	Yes	Yes	No	No	No	No	No

IPv6 Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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 ACLs	Extended ACLs	Yes	Yes	No	No	No	No	No
IPv6 Routing Protocols	RIPng IS-IS for IPv6 OSPFv3 IPsec Authentication BGP4+	Yes	Yes	No	No	No	No	No
IPv6 Multicast Routing	MLD v1, v2 PIM-SSM PIM-SM Anycast RP	Yes	Yes	No	No	No	No	No

MPLS Features Supported

Category	Feature description	NetIron XMR Series	NetIron MLX 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
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 the NetIron XMR Series and NetIron MLX Series

The following features are not supported in software release 04.1.00b on NetIron XMR series and NetIron MLX 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 in the NetIron CES series and NetIron CER series

The following features are not supported in software release 04.1.00b on NetIron CES series and NetIron CER series routers:

- IPv6
- 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
- MPLS Layer 3 VPNs
- Web Based GUI
- Hot swapping of 10-Gig modules

Not Applicable features in the NetIron CES series and NetIron CER series

The following features are not applicable in software release 04.1.00b on NetIron CES series and NetIron CER series routers:

- Hitless Management Failover
- Hitless Upgrade

- Packet Over SONET (POS)

Image Files in Multi-Service IronWare Release 04.1.00b for the NetIron XMR and NetIron MLX Series

The following software image files are available for Multi-Service IronWare release 04.1.00b for the NetIron XMR series or NetIron MLX series routers.

Image Files for Management and Interface Modules		
Module	**Image Type**	**Image name**
Management & Interface Modules for: NetIron MLX-4, NetIron MLX-8, NetIron MLX-16, and NetIron MLX-32 NetIron XMR 4000, NetIron XMR 8000, NetIron XMR 16000, and NetIron XMR 32000	IronWare (combined image)	xm04100b Note: Recommended
Management Modules for: NetIron MLX-4, NetIron MLX-8, NetIron MLX-16, and NetIron MLX-32 NetIron XMR 4000, NetIron XMR 8000, NetIron XMR 16000, and NetIron XMR 32000	Monitor	xmb04100b
	Boot	xmprm03500
	Ironware	xmr04100b
Management Modules for: NetIron MLX-4, NetIron MLX-8, and NetIron MLX-16 NetIron XMR 4000, NetIron XMR 8000, and NetIron XMR 16000	FPGA	mbridge See table “FPGA Image Files for Management Modules”
Management Modules for: NetIron MLX-32 and NetIron XMR 32000		mbridge32 See table “FPGA Image Files for Management Modules”
Interface Modules	Monitor	xmlb04100b
	Boot	xmlprm03500
	Ironware	xmlp04100b
	FPGA (Combined Image)	lpfpga04100b
Interface Modules	FPGA (Individual Images)	pbifsp2 See "PBIFSP2.bin" in table “FPGA Image Files for Interface Modules”
		xppsp2 See "XPPSP2.bin" in table “FPGA Image Files for Interface Modules”

Image Files for Management and Interface Modules		
Module	**Image Type**	**Image name**
		xgmacsp2 (only used on 10 G interface module) See "XGMACSP2.bin" in table "FPGA Image Files for Interface Modules"
		xppoc (only used on POS interface modules) See "XPPOC.bin" in table "FPGA Image Files for Interface Modules"
		pbifoc (only used on POS interface modules) See "PBIFOC.bin" in table "FPGA Image Files for Interface Modules"
		statsoc (only used on POS interface modules) See "STATSOC.bin" in table "FPGA Image Files for Interface Modules"
		pbifmrj (Mini-RJ only) See "PBIFMRJ.bin" in table "FPGA Image Files for Interface Modules"
		xppmrj (Mini-RJ only) See "XPPMRJ.bin" in table "FPGA Image Files for Interface Modules"
		statsmrj (Mini-RJ only) See "STATSMRJ.bin" in table "FPGA Image Files for Interface Modules"
Switch Fabric Modules MLX-32 and XMR 32000 only	FPGA	sbridge See table "FPGA Image Files for Switch Fabric Modules"

NOTE: The software described in these notes applies only to the NetIron MLX Series and NetIron XMR Series routers. You cannot use this software on other Brocade devices.

FPGA Images for Multi-Service IronWare Release 04.1.00

You must have the correct FPGA images loaded on your router to run the software. The following table describes the FPGA versions required on the management modules to run the listed software releases for NetIron MLX Series and NetIron XMR Series routers.

FPGA Image Files for Management Modules (NetIron MLX-4, NetIron MLX-8, NetIron MLX-16, NetIron XMR 4000, NetIron XMR 8000, and NetIron XMR 16000)			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Module Supported**
03.9.00	MBRIDGE	21	Management module
03.9.01		21	Management module
04.0.00 through 04.0.01		21	Management module
04.1.00 through 04.1.00b		21	Management module

FPGA Image Files for Management Modules (NetIron MLX-32 and NetIron XMR 32000)			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Module Supported**
03.9.00	MBRIDGE32	21	Management module
03.9.01		21	Management module
04.0.00 through 04.0.01		21	Management module
04.1.00 through 04.1.00b		21	Management module

NOTE: 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 of both active and standby management modules before starting the upgrade process. The upgrade may fail if this procedure is not followed.

FPGA Image Files for Interface Modules			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Interface Module Supported**
04.1.00b	lpfpga04100b.bin	FPGA (combined) for all Interface Modules	
03.9.00	PBIFSP2.bin	3.08	All Ethernet Modules (except for Mini-RJ)
03.9.01		3.10	All Ethernet Modules (except for Mini-RJ)

FPGA Image Files for Interface Modules			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Interface Module Supported**
04.0.00 through 04.0.01		3.14	All Ethernet Modules (except for Mini-RJ)
04.1.00 through 04.1.00b		3.14	All Ethernet Modules (except for Mini-RJ)
03.9.00	XPPSP2.bin	4.05	All Ethernet Modules (except for Mini-RJ)
03.9.01		4.05	All Ethernet Modules (except for Mini-RJ)
04.0.00 through 04.0.01		5.07	All Ethernet Modules (except for Mini-RJ)
04.1.00 through 04.1.00b		5.22	All Ethernet Modules (except for Mini-RJ)
03.9.00	XGMACSP2.bin	0.11	10 GbE Modules only
03.9.01		0.11	10 GbE Modules only
04.0.00 through 04.0.01		0.12	10 GbE Modules only
04.1.00 through 04.1.00b		0.12	10 GbE Modules only
03.9.00	XPPOC.bin	3.31	POS Modules only
03.9.01		3.31	POS Modules only
04.0.00 through 04.0.01		5.07	POS Modules only
04.1.00 through 04.1.00b		5.08	POS Modules only
03.9.00	PBIFOC.bin	3.03	POS Modules only
03.9.01		3.03	POS Modules only
04.0.00 through 04.0.01		3.04	POS Modules only
04.1.00 through 04.1.00b		3.05	POS Modules only
03.9.00	STATSOC.bin	2.06	POS Modules only
03.9.01		2.06	POS Modules only

FPGA Image Files for Interface Modules			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Interface Module Supported**
04.0.00 through 04.0.01		2.06	POS Modules only
04.1.00 through 04.1.00b		2.06	POS Modules only
04.0.00 through 04.0.01	PBIFMRJ.bin	3.13	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only
04.1.00 through 04.1.00b		3.14	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only
04.0.00 through 04.0.01	XPPMRJ.bin	5.07	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only
04.1.00 through 04.1.00b		5.09	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only
04.0.00 through 04.0.01	STATSMRJ.bin	0.07	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only
04.1.00 through 04.1.00b		0.07	NI-MLX-1Gx48-T and NI-MLX-1Gx48-T-A (Mini-RJ) only

FPGA Image Files for Switch Fabric Modules (NetIron MLX-32 and NetIron XMR 32000)			
Software Image Installed	**FPGA Image**	**Compatible FPGA Version**	**Module Supported**
03.9.00	SBRIDGE	6	Management module
03.9.01		6	Management module
04.0.00 through 04.0.01		6	Management module
04.1.00 through 04.1.00b		6	Management module

Software is loaded at the factory.

NOTE: The FPGA images described here for use with the NetIron MLX Series and NetIron XMR Series routers differ from those used for other NetIron platforms such as the NetIron IMR 640 or NetIron 40G routers.

Upgrading Software on the NetIron XMR and NetIron MLX Series

Important Notes before Upgrading the Software

Read this section before attempting to upgrade the NI-MLX-1Gx48-T interface modules. When upgrading or downgrading from or to software versions 3.5 and earlier, please refer to the *Multi-Service IronWare Software Release 04.0.00 for Brocade NetIron XMR and NetIron MLX, Release Notes v1.0* for appropriate procedures.

NOTE: If a NetIron MLX or NetIron XMR router contains POS interface modules, it should not be downgraded to a Multi-Service IronWare software release earlier than 03.4.00.

The NetIron MLX-32 and NetIron XMR 32000 should not be downgraded to a Multi-Service IronWare software release earlier than 03.6.00.

Considerations for Downgrading from 04.1.00

Downgrading from release 04.1.00 to an earlier release of the software can impact IPv6 routing. IPv6 routing is enabled by default in release 04.1.00 and therefore does not appear in the configuration. If you are downgrading from 04.1.00 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.

Considerations for Upgrading to 04.0.00 and Later

When upgrading to release 04.0.00 and later, consider the changes to the following:

- ifIndex Allocation
- Port MAC Address Change
- QoS Priorities for NI-MLX-1Gx48-T Modules

ifIndex Allocation

SNMP Management Information Base (MIB) uses Interface Index (ifIndex) to assign a unique value to each port on a module or slot. Beginning with release 04.0.00, 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 release 04.0.00, consider the following:

- If you are running 03.9.00 or earlier and you will be installing the NI-MLX-1Gx48-T module on you NetIron MLX, 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 status remains in the Offline state.
- If you are running 03.9.00 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 NetIron MLX (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 NetIron MLX (no previous software installed), but 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 in case an NI-MLX-1Gx48-T module is installed in the future.

Port MAC Address Change

Beginning with release 04.0.00, the MAC address assigned to each port may change to accommodate more number of ports per module. The total MAC address allocated for each module has increased from 20 to 48 ports per module.

QoS Priorities for NI-MLX-1Gx48-T Modules

Beginning with release 04.0.00, the NetIron configuration allows you configure more ports in the system by changing the QoS priorities from 8 to 4 priorities per port. This enables the NetIron chassis to support 2016 ports using 4 priorities per port.

Using Older Software on Interface Modules in a 32-Slot Chassis

The NetIron XMR 32000 and MLX-32 chassis can use interface modules that have older versions of the Multi-Service IronWare software installed on them. For special considerations in the use of older software in a 32-slot chassis, please consult *Multi-Service IronWare Software Release 04.0.01 for Brocade NetIron XMR and NetIron MLX Release Notes v1.0*.

Using Unified Images

To simplify Multi-Service IronWare upgrades, we have reduced the number of files needed to upgrade a NetIron XMR or NetIron MLX router as described:

- A single-bundled IronWare image now contains both Management Module and Interface Module IronWare images. Using this single-bundled image: simplifies upgrading the system, reduces the chance of operator error and ensures that image versions on all the management modules and interface modules are consistent. Please note that you must be upgrading from a 03.5.00 or later image to a 03.5.00 or later image before you can take advantage of this feature
- Boot images no longer need to be upgraded with each release and in fact will almost never need to be changed. This eliminates one extra step in the upgrade process, thus simplifying the upgrade procedure, reducing the chance of operator error and leading to a faster upgrade process.
- The Monitor image no longer needs to be upgraded with each release. All OS functions have been moved out of the Monitor image into the IronWare image. This has simplified the Monitor image and it no longer needs to be upgraded every time, thus eliminating another step in the upgrade process. Please note that you must be upgrading from a 03.5.00 or later image to a 03.5.00 or later image before you can take advantage of this feature.

Images and Procedures Required for the NetIron XMR and NetIron MLX Series

If updating to or from Multi-Service IronWare releases before 03.5.00, please refer to the *Multi-Service IronWare Software Release 04.0.00 for Brocade NetIron XMR and NetIron MLX Release Notes v1.0.* For later releases, the software images required and the procedures for upgrading are described in the following sections:

- Description of the Images Required – This sub-section describes each of the images required to operate a NetIron MLX series or NetIron XMR series router.
- Software Upgrade and Downgrade Considerations for Releases 03.5.00 and Before
- Displaying Flash Memory and Version Information – This sub-section describes the commands that allow you to determine the contents of the NetIron MLX Series or NetIron XMR Series router's flash memory and how to read the output of those commands.
- Upgrading the IronWare Image – This sub-section describes the procedures required for upgrading the Management and Interface module's IronWare software image together. Also described are procedures for upgrading the Management module software IronWare image and upgrading the Interface module software IronWare image.
- Upgrading the Monitor and Boot Images on a Management Module – This sub-section describes the procedures required for upgrading the Monitor and Boot software images on a Management module. The procedures described apply to all versions of the software.
- Upgrading the Monitor and Boot Images on an Interface Module – This sub-section describes the procedures required for upgrading the Monitor and Boot software images on an Interface module. The

procedures described apply to all versions of the software.

- Upgrading the MBRIDGE FPGA Image on a Management Module – This sub-section describes the procedures required for upgrading the MBRIDGE FPGA image on a Management module.
- Upgrading the FPGA Image on an Interface Module – This section describes the procedures required for upgrading the FPGA images on an Interface Module.
- Rebooting the Management Module – This sub-section describes the procedures required for rebooting the Management Module after upgrading the software images.
- Hitless OS Upgrade – This sub-section describes the procedures required for performing a Hitless OS Upgrade. Using Hitless OS upgrade, you can upgrade the Multi-Service IronWare software without a loss of service or disruption to some functions and protocols.
- Software Image Coherence Check – This sub-section describes the procedures for ensuring that the router is installing compatible versions of all images on the Management and Interface modules.

Description of the Software Images Required

The functionality within each of the software images required to operate the NetIron MLX or NetIron XMR is described in the table below. Because the functions that are most likely to change are contained within the IronWare image, updates will usually only require updating the IronWare image.

Software Image	Function	Management Module Image Name	Interface Module Image Name
Boot Image	Bootstrap	xmprm<xxxx>	xmlprm<xxxx>
Monitor Image	Image Handling Memory Init	xmb<xxxx>	xmlb<xxxx>
IronWare Image	Application OS	xmr<xxxx>	xmlp<xxxx>

Software Upgrade and Downgrade Considerations for Releases 03.5.00 and Before

For software releases 03.5.00 and before, there are special considerations when:

- Upgrading from version 03.5.00 (or later) to a later version
- Upgrading to version 03.5.00 (or later) from a pre-03.5.00 version
- Downgrading from version 03.5.00 (or later) to a pre-03.5.00 version

For a detailed treatment of these issues, please see *Multi-Service IronWare Software Release 04.0.01 for Brocade NetIron XMR and NetIron MLX Release Notes v1.0*.

Displaying Flash Memory and Version Information

Prior to upgrading the images on a NetIron MLX or NetIron XMR router, it is advisable to check the versions already installed. This allows you to determine which versions need to be upgraded. It is also advisable to check the versions installed immediately after an upgrade to confirm the upgraded software versions. The following sections describe how to use the **show flash** and **show version** commands to display this information.

Displaying Flash Information

You can display information concerning the contents of a NetIron MLX Series or NetIron XMR Series router using the **show flash** command as shown in the following:

```
NetIron# show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Active Management Module (Left Slot)
Code Flash - Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 4.1.0bT163, Size 5362583 bytes, Check Sum c856
    Compiled on Mar 11 2010 at 20:36:44 labeled as xmr04100b
  o LP Kernel Image (Monitor for LP Image Type 0)
    Version 4.1.0bT175, Size 422399 bytes, Check Sum e57e
    Compiled on Feb 26 2010 at 18:34:18 labeled as xmlb04100b
  o LP IronWare Image (Primary for LP Image Type 0)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o LP IronWare Image (Secondary for LP Image Type 0)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o Monitor Image
    Version 4.1.0bT165, Size 464413 bytes, Check Sum 894a
    Compiled on Feb 26 2010 at 18:33:34 labeled as xmb04100b
  o Startup Configuration
    Size 1286 bytes, Check Sum ed89
    Modified on 14:56:08 Pacific Tue Mar 16 2010

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 3.5.0T165, Size 424484 bytes, Check Sum b751
    Compiled on Jul 10 2007 at 19:13:56 labeled as xmprm03500
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Line Card Slot 2
Code Flash: Type MT28F640J3, Size 16 MB
  o IronWare Image (Primary)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o IronWare Image (Secondary)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o Monitor Image
    Version 4.1.0bT175, Size 422399 bytes, Check Sum e57e
    Compiled on Feb 26 2010 at 18:34:18 labeled as xmlb04100b
Boot Flash: Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 3.5.0T175, Size 387133 bytes, Check Sum d63d
    Compiled on Jul 10 2007 at 19:14:32 labeled as xmlprm03500
FPGA Version (Stored In Flash):
 PBIF Version = 3.14, Build Time = 12/17/2008 14:32:00

 XPP Version = 5.22, Build Time = 8/6/2009 19:10:00

 XGMAC Version = 0.12, Build Time = 11/10/2008 15:50:00
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
All show flash done
```

This Field...	Displays...
Management Modules	
<type> Management Module (<location>)	The management module for which flash information is displayed. <type> indicates an active or standby management module. <location> indicates the top or bottom slot (M1 or M2, respectively).
Code Flash	The model number and size of the management module's code flash.
IronWare Image (Primary or Secondary)	Indicates the IronWare image installed in the primary or secondary location in the management module's code flash. The image must be **xmr<xxxxx>**. The actual image name depends on the version of software you have running on your router. The output displays the following information about the image: • Version – "**4.1.0b***Txxy*" indicates the image version number. "*xx*" indicates the hardware type; "*y*" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.
Line Processor (LP) Kernel Image (Monitor for LP Image Type 0)	Indicates the interface modules Monitor image stored in the management module's code flash. The image must be **xmlb<xxxxx>**. The management module stores these images only; it does not run the images. The output displays the following information about the image: • Version – "**4.1.0b***Txxy*" indicates the image version number. "*xx*" indicates the hardware type; "*y*" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.
LP IronWare Image (Primary or Secondary for LP Image Type 0)	Indicates the interface modules' primary and/or secondary IronWare image stored in the management module's code flash if you copied the primary and/or secondary IronWare image to all interface modules using the **copy** command with the **all** keyword. The management module stores these images only; it does not run the images. The image must be **xmlp<xxxxx>.** The output displays the following information about the image: • Version – "**4.1.0b***Txxy*" indicates the image version number. "*xx*" indicates the hardware type; "*y*" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.

This Field...	Displays...
Monitor Image	Indicates the monitor image installed in the management module's code flash. The image must be **xmb<xxxxx>**. The output displays the following information about the image: • Version – "**4.1.0b*Txxy***" indicates the image version number. "***xx***" indicates the hardware type; "***y***" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.
Startup Configuration	The output displays the following information about the startup configuration, which is saved in the management module's code flash: • Size – Size, in bytes, of the startup configuration. • Check sum – A unique ID for the file. If the contents of the file change, the check sum changes also. • Modification date and time – Date and time that the startup configuration was last saved.
Boot Flash	The model number and size of the management module's boot flash.
Boot Image	Indicates the boot image installed in the management module's boot flash. The image must be **xmprm<xxxxx>.** The output displays the following information about the image: • Version – **" 3.5.0*Txxy***" indicates the image version number. "***xx***" indicates the hardware type; "***y***" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.
Interface Modules	
Line Card Slot <number>	The interface module for which flash information is displayed. The <number> parameter indicates the number of the chassis slot, 1 – 16, in which the interface module is installed.
Code Flash	The model number and size of the interface module's code flash.
IronWare Image (Primary or Secondary)	Indicates the IronWare image installed in the primary or secondary location in the interface module's code flash. The image must be **xmlp<xxxxx>**. The output displays the following information about the image: • Version – "**4.1.0b*Txxy***" indicates the image version number. "***xx***" indicates the hardware type; "***y***" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.

This Field...	Displays...
Monitor Image	Indicates the monitor image installed in the interface module's code flash. The image must be **xmlb<xxxxx>**. The output displays the following information about the image: • Version – "**4.1.0b***Txxy*" indicates the image version number. "*xx*" indicates the hardware type; "*y*" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.
Boot Flash	The model number and size of the interface module's boot flash.
Boot Image	Indicates the boot image installed in the interface module's boot flash. The image must be **xmlprm<xxxxx>**. The output displays the following information about the image: • Version – " **3.5.0***Txxy*" indicates the image version number. "*xx*" indicates the hardware type; "*y*" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that the image was compiled.

This Field...	Displays...
FPGA Version Information	The output displays the following information about the field-programmable gate array (FPGA) images that is stored in Flash for installation on the interface modules: • **PBIF** image information – The version number of the PBIF image. This image is installed on both Ethernet and POS Interface modules but from different image files. The versions installed on Ethernet and POS Interface modules can differ and should reflect the correct image for your release. • **XPP** image information – The version number of the XPP image. This image is installed on both Ethernet and POS Interface modules but from different image files. The versions installed on Ethernet and POS Interface modules can differ and should reflect the correct image for your release. • **STATS** image information – The version number of the STATS image. This image is only installed on POS Interface modules. • **XGMAC** image information – The version number of the XGMAC image. This image is only installed on the 10 Gbps interface module. **NOTE:** The FPGA version installed on your module should be the correct one for the version of Multi-Service IronWare you are running. Images compatible with each version and Interface module are described in the section "FPGA Images for Multi-Service IronWare Release 04.1.00." The following Images are only displayed from the **show version** command: • **MBRIDGE** Revision – The version number of the MBRIDGE FPGA installed on the Management module. The MBRIDGE FPGA is not used on Management modules for the NetIron MLX-32 or NetIron XMR 32000 chassis. • **MBRIDGE32** Revision – The version number of the MBRIDGE32 FPGA installed on the Management module. The MBRIDGE32 FPGA is only used on Management modules for the NetIron MLX-32 or NetIron XMR 32000 chassis. • **SBRIDGE** Revision – The version number of the SBRIDGE FPGA installed on the NetIron MLX-32 or NetIron XMR 32000 Switch Fabric modules.

Displaying Version Information

You can display version information for a NetIron MLX Series or NetIron XMR Series router using the **show version** command as shown in the following:

```
NetIron(config)# show version
HW: NetIron XMR 4K Router
Chassis (Serial #: SA18065027,  Part #: 31550-000B)
NI-X-SF Switch Fabric Module 1 (Serial #: SA18060320,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
NI-X-SF Switch Fabric Module 2 (Serial #: SA18060446,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
NI-X-SF Switch Fabric Module 3 (Serial #: SA18060389,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
==========================================================================
SL M1: NI-MLX-MR Management Module Active (Serial #: SA21060514, Part #: 31524-500B):
Boot     : Version 3.5.0T165 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jul 10 2007 at 19:13:56 labeled as xmprm03500
```

```
 (424484 bytes) from boot flash
Monitor  : Version 4.1.0bT165 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Feb 26 2010 at 18:33:34 labeled as xmb04100b
 (464413 bytes) from code flash
IronWare : Version 4.1.0bT163 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 11 2010 at 20:36:44 labeled as xmr04100b
 (5362583 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 21
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
2048 MB DRAM
Active Management uptime is 3 minutes 10 seconds
========================================================================
SL 2: NI-XMR-10Gx2 2-port 10GbE Module (Serial #: pr32050028, Part #: 31546-100A)
Boot     : Version 3.5.0T175 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jul 10 2007 at 19:14:32 labeled as xmlprm03500
 (387133 bytes) from boot flash
Monitor  : Version 4.1.0bT175 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Feb 26 2010 at 18:34:18 labeled as xmlb04100b
 (422399 bytes) from code flash
IronWare : Version 4.1.0bT177 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
 (3679308 bytes) from Primary
FPGA versions:
Valid PBIF Version = 3.14, Build Time = 12/17/2008 14:32:00

Valid XPP Version = 5.22, Build Time = 8/6/2009 19:10:00

Valid XGMAC Version = 0.12, Build Time = 11/10/2008 15:50:00

X10G2MAC 0
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, 286331153 Bytes BRAM
PPCR0: 1024K entries CAM, 16384K PRAM, 2048K AGE RAM
LP Slot 2 uptime is 2 minutes 45 seconds
========================================================================
All show version done
```

Syntax: show version

The highlighted lines in the output indicate the versions currently running boot, monitor, IronWare and FPGA images for the management, interface and switch fabric modules.

Upgrading the IronWare Image

Upgrading the IronWare Images on the Management and Interface Modules Together

You can download a single **xm<*xxxxx*>** file that contains the **xmr<*xxxxx*>** and **xmlp<*xxxxx*>** files for both the Management and Interface modules using the **copy tftp image** command.

NOTE: You can also download IronWare images using the secure copy feature as described in the *NetIron Configuration Guide*.

The combined image never upgrades an FPGA. If an FPGA upgrade is required for a release, you must use the **copy tftp lp** command to download the new FPGA image to the Interface module as described for earlier releases.

NOTE: If you are upgrading from a pre-03.5.00 version or downgrading to a pre-03.5.00 release, you must use the **copy tftp flash** and **copy tftp lp** commands.

To upgrade the IronWare images to the Management and Interface modules using a single command, you must place the consolidated IronWare image (**xm**<*xxxxx*>) on a TFTP server that the router has access and execute the following command:

```
NetIron# copy tftp image 10.10.10.10 xm03500.bin
```

Syntax: **copy tftp image** <*IP-address*> <*image-name*> [**lp-sec** | **mp-sec** | **secondary**]

The <*IP-address*> variable specifies the address of the TFTP server that contains the **xm**<*xxxxx*> software image that you want to download to the router. The default command copies the **xmr**<*xxxxx*> and **xmlp**<*xxxxx*> files in the specified **xm**<*xxxxx*> software image to the primary management module image and the primary interface module image.

The following options change the destination for the **xmr**<*xxxxx*> and **xmlp**<*xxxxx*> files downloaded to the router as described:

- Using the **secondary** option with the command copies the **xmr**<*xxxxx*> and **xmlp**<*xxxxx*> files in the specified **xm**<*xxxxx*> software image to the secondary management module image and the secondary interface module image.
- Using the **lp-sec** option with the command copies the **xmr**<*xxxxx*> file in the specified **xm**<*xxxxx*> software image to the primary management module image while copying the **xmlp**<*xxxxx*> file to the secondary interface module image.
- Using the **mp-sec** option with the command copies the **xmr**<*xxxxx*> file in the specified **xm**<*xxxxx*> software image to the secondary management module image while copying the **xmlp**<*xxxxx*> file to the primary interface module image.

Upgrading the IronWare Image on a Management Module

To upgrade the management module's IronWare image (primary or secondary) individually, you must perform the following steps:

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

NOTE: Lack of available flash memory is typically only seen in a 32-slot chassis.

1. Verify that you have enough available "bytes free" in the flash memory before you begin the upgrade procedure by entering the following command:

   EXAMPLE:

```
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
```

2. You can delete the **mbridge.old** file to increase the available "bytes free." Though unlikely, you may have to remove additional files in order for the upgrade to succeed. Please contact your vendor support for guidance on removal of additional files.

NOTE: You must have three underscores in the file name: delete___mbridge.old.

```
NetIron#delete___mbridge.old
```

3. After deleting the **mbridge.old** file, check the directory again to verify that the **mbridge.old** file has been removed, and that there are enough bytes free to begin the upgrade procedure. Enter the following command:

```
Standby MP#directory
```

EXAMPLE:

```
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
```

4. If you have a redundant Management module, the same procedure needs to be applied. In order to access your redundant Management module, you will need to execute the switchover command to make it active.

5. Enter the following command:

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

6. You are asked to verify this command. Enter '**y**'.

7. Once you have deleted the file and noted the available "bytes free," execute the switchover command again to make the original Management module the active one.

You can now follow the procedures to upgrade the Multi-Service IronWare.

1. Place the new IronWare image on a TFTP server to which the router has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new IronWare image from the TFTP server or a flash card in slot 1 or 2 to the management module's code flash or a flash card in slot 1 or 2. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI:

- **copy tftp flash** <ip-addr> <image-name> **primary | secondary**
- **copy tftp slot1 | slot2** <ip-addr> <image-name> **primary | secondary**
- **copy slot1 | slot2 flash** <image-name> **primary | secondary**
- **copy slot1 | slot2 slot1 | slot2** <image-name> <dest-name>

For information about the image name to specify, see table above.

3. Verify that the new IronWare 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.
4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process. For more information, see "Rebooting the Management Module."

Upgrading the IronWare Image on an Interface Module

To upgrade an IronWare image (primary or secondary) on all interface modules or an interface module in a specified chassis slot, perform the following steps:

1. Place the new IronWare image on a TFTP server that the router has access or on a PCMCIA flash card inserted in slot 1 or 2.
2. Copy the new IronWare image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (example: NetIron#):
   - **copy tftp lp** <ip-addr> <image-name> **primary | secondary all**
   - **copy tftp lp** <ip-addr> <image-name> **primary | secondary** <chassis-slot-number>
   - **copy slot1 | slot2 lp** <image-name> **primary | secondary all**
   - **copy slot1 | slot2 lp** <image-name> **primary | secondary** <chassis-slot-number>

   For information about the image name to specify, see "Software Image Files for Multi-Service IronWare R04.1.00."

   NOTE: If you copy the new IronWare image to all interface modules using the **all** keyword, the management module makes a copy of the image (called lp-primary-0 or lp-secondary-0) and stores it in its code flash, thereby synchronizing the new IronWare image on both the interface and management modules.

   If you copy the new IronWare image to a specified chassis slot, the management module does not make a copy of the image or store it. In this case, the new IronWare image on the interface module is unsynchronized or different from the IronWare image on the management module.

   For more information about synchronizing the new IronWare image or retaining unsynchronized versions of the IronWare image on the interface and management modules, see "Rebooting the Management Module."
3. Verify that the new IronWare image has been successfully copied by entering the following command at any level of the CLI:

   show flash

   Check for the IronWare image and the date and time at which the image was built.

If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process. For more information, see "Rebooting the Management Module" below.

Upgrading the Monitor and Boot Images on a Management Module

To upgrade a Management Module's monitor and boot images, perform the following steps:

1. Place the new monitor and boot images on a TFTP server to which the router has access or on a PCMCIA flash card inserted in slot 1 or 2.
2. Copy the new monitor and boot images to the router. Enter one of the following commands at the Privileged EXEC level of the CLI (example: `NetIron#`):

Command Syntax	Description
copy tftp flash <ip-addr> <image-name> **monitor**	Copies the latest monitor image from the TFTP server to flash.
copy tftp flash <ip-addr> <image-name> **boot**	Copies the latest boot image from the TFTP server to flash.
copy slot1 | slot2 flash <image-name> **monitor**	Copies the latest monitor image from a flash card in slot 1 or 2 to flash.
copy slot1 | slot2 flash <image-name> **boot**	Copies the latest boot image from a flash card in slot 1 or 2 to flash.

   For information about the image name to specify, see the image table.
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>/** (if the destination is slot 1 or 2)

   Check for the boot image, monitor image, and the date and time at which the new images were built.
4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process.

Upgrading the Monitor and Boot Images on an Interface Module

NOTE: We recommend that you perform this upgrade procedure from a PC or terminal that is directly connected to the management module's Console port. You can also perform this procedure via a Telnet or SSHv2 session.

When upgrading from a pre-03.5.00 version to version 03.5.00 (or later), you must upgrade the monitor and boot images at the same time as the IronWare image.

If you are upgrading from version 03.5.00 or later to a later version, you should only upgrade the monitor and boot images as described in the relevant release notes.

To upgrade an interface's monitor and boot images, perform the following steps:

1. Place the new monitor and boot images on a TFTP server to which the router has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new monitor and boot images to the router. Enter the following commands at the Privileged EXEC level of the CLI (example: `NetIron#`):

Command Syntax	Description
copy tftp lp <ip-addr> <image-name> **monitor all** | <slot-number>	Copies the latest monitor image from the TFTP server to all interface modules or to the specified interface module (slot-number).
copy tftp lp <ip-addr> <image-name> **boot all** | <slot-number>	Copies the latest boot image from the TFTP server to all interface modules or to the specified interface module (slot-number).

For information about the image name to specify, see table above.

3. Verify that the new images were successfully copied to code flash by entering the following command at the Privileged EXEC level of the CLI:

   - **show flash**

   Check for the monitor image, boot image, and the date and time at which the new images were built.

4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process.

Upgrading the MBRIDGE FPGA Image on a Management Module

NetIron MLX Series and NetIron XMR Series Management modules contain an upgradeable FPGA image called MBRIDGE.

The MBRIDGE image installed must be compatible with the software version you are running on the router. Please see "FPGA Images for Multi-Service IronWare Release 04.1.00" for tables of which FPGA images are required for each software version.

NOTE: You will not need to upgrade the MBRIDGE FPGA image with every Multi-Service software upgrade. Only upgrade this image if specified in the release notes.

Overview of Tasks in the FPGA Image Upgrade Process

To upgrade the MBRIDGE FPGA image on a Management module, you must perform the following general steps:

1. Determine the versions of the images currently installed on the Management module.

   For information about performing this task, see "Determining the MBRIDGE Image Versions."

2. Copy the new image from a source to a destination.

   The source from which to copy the new image must be a TFTP server to which the router has access or a flash card in the management module's slot 1 or 2. The destination to which to copy the new image is all or one specified interface module.

   For information about performing this task, see "Upgrading the MBRIDGE FPGA Image."

3. Reboot the management module upon which you upgraded the MBRIDGE images.

Determining the MBRIDGE Image Versions

To display the versions of the MBRIDGE images currently installed on the Gigabit Ethernet modules, enter the **`show version`** command at any level of the CLI:

```
NetIron(config)# show version
HW: NetIron XMR 4K Router
```

```
Chassis (Serial #: SA18065027,  Part #: 31550-000B)
NI-X-SF Switch Fabric Module 1 (Serial #: SA18060320,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
NI-X-SF Switch Fabric Module 2 (Serial #: SA18060446,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
NI-X-SF Switch Fabric Module 3 (Serial #: SA18060389,  Part #: 31548-000B)
FE 1: Type fe200,  Version 2
======================================================================
SL M1: NI-MLX-MR Management Module Active (Serial #: SA21060514, Part #: 31524-500B):
Boot     : Version 3.5.0T165 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jul 10 2007 at 19:13:56 labeled as xmprm03500
 (424484 bytes) from boot flash
Monitor  : Version 4.1.0bT165 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Feb 26 2010 at 18:33:34 labeled as xmb04100b
 (464413 bytes) from code flash
IronWare : Version 4.1.0bT163 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 11 2010 at 20:36:44 labeled as xmr04100b
 (5362583 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 21
916 MHz Power PC processor 7447A (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
2048 MB DRAM
Active Management uptime is 3 minutes 10 seconds
======================================================================
```

The highlighted lines in the output indicate that the management module currently has MBRIDGE Revision: 21 installed.

Upgrading the MBRIDGE FPGA Image

To upgrade one or more MBRIDGE FPGA images on Management modules within a NetIron XMR or NetIron MLX chassis, perform the following steps:

1. Place the new MBRIDGE FPGA image on a TFTP server to which the router has access or on a PCMCIA flash card inserted in slot 1 or 2.
2. Copy the MBRIDGE FPGA image from the TFTP server or a flash card in slot 1 or 2 to all management modules. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (for example: NetIron#):
   - **copy tftp mbridge** <ip-addr> <image-name>
   - **copy slot1 | slot2 mbridge** <image-name>
3. Verify that the MBRIDGE image(s) have been successfully copied to the management module(s) by entering the following command at any level of the CLI:
   - **show version**

   Check for the MBRIDGE image version numbers in the output.

Upgrading the FPGA Image on an Interface Module

Ethernet interface modules contain the following upgradeable field-programmable gate array (FPGA) images:

- PBIF
- XPP
- XGMAC (10 Gbps Interface Modules Only)

Packet Over SONET (POS) interface modules contain the following upgradeable field-programmable gate array (FPGA) images:

- XPPOC
- PBIFOC
- STATSOC

48-port mini RJ-21 interface modules contain the following upgradeable field-programmable gate array (FPGA) images:

- PBIFMRJ
- XPPMRJ
- STATSMRJ

The FPGA images installed must be compatible with the software version you are running on the router. “FPGA Images for Multi-Service IronWare Release 04.1.00” maps the compatibility of FPGA images to Software versions.

The process for upgrading FPGA images is enhanced to allow you to upgrade FPGA images for all NetIron interface modules at the same time. This enhancement provides an easier upgrade process by allowing you to upgrade all FPGA images in all interface modules using one CLI. For each release there is a corresponding bundled FPGA image release.

When the bundled FPGA image is copied (via TFTP or PCMCIA) into the NetIron system, the bundled image is parsed by the Management Module. The Management Module selects only applicable individual images to be downloaded into the Interface Module. The applicable images are determined based on the card types that are plugged into the system. The images are checked for any duplicates before downloading into the Interface Modules.

Overview of Tasks in the FPGA Image Upgrade Process

To upgrade the FPGA images on the interface modules, you must perform the following general steps:

1. Determine the versions of the images currently installed on the interface modules.

   For information about performing this task, see “Determining the FPGA Versions.”

2. Copy the new image from a source to a destination.

   The source from which to copy the new image is usually a TFTP server to which the router has access or a flash card in the management module’s slot 1 or 2. The destination to which to copy the new image can be one of the following:

   - All slots in the chassis
   - All slots with a specified Module type
   - A specific slot number

   You can choose to upgrade FPGA Images in either of two ways:

   - You can upgrade all LP FPGA images at the same time. For information about performing this task, see “Upgrading all LP FPGA Images for all Interface Modules at the Same Time.”
   - You can upgrade FPGA images one image at a time. For information about performing this task, see “Upgrading the FPGA Images One Image at a Time.”

3. Reboot the interface module upon which you upgraded the FPGA images.

Duplicate FPGA Download Prevention

The FPGA upgrade utility has been enhanced to help eliminate unnecessary FPGA upgrades by having the system compare the FPGA image version currently saved on flash to any new images being downloaded. If the versions are identical, the download is aborted and a Warning message is sent. If you want to upgrade an identical image, you can use the **force-overwrite** option with the FPGA upgrade command. Operation of this feature is described in detail below.

Determining the FPGA Image Versions

To display the versions of the FPGA images currently installed on the Gigabit Ethernet modules, enter the following command at any level of the CLI:

```
NetIron#show flash
...
Line Card Slot 2
Code Flash: Type MT28F640J3, Size 16 MB
  o IronWare Image (Primary)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o IronWare Image (Secondary)
    Version 4.1.0bT177, Size 3679308 bytes, Check Sum ff12
    Compiled on Mar 11 2010 at 20:45:14 labeled as xmlp04100b
  o Monitor Image
    Version 4.1.0bT175, Size 422399 bytes, Check Sum e57e
    Compiled on Feb 26 2010 at 18:34:18 labeled as xmlb04100b
Boot Flash: Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 3.5.0T175, Size 387133 bytes, Check Sum d63d
    Compiled on Jul 10 2007 at 19:14:32 labeled as xmlprm03500
FPGA Version (Stored In Flash):
 PBIF Version = 3.14, Build Time = 12/17/2008 14:32:00

 XPP Version = 5.22, Build Time = 8/6/2009 19:10:00

 XGMAC Version = 0.12, Build Time = 11/10/2008 15:50:00

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

The highlighted lines in the output indicate that the interface module in chassis slot 1 currently has PBIF version 3.14 and XPP version 5.22 installed.

Upgrading All LP FPGA Images at the Same Time

WARNING: You must use an FPGA images that is specified for the NetIron MLX Series or NetIron XMR Series routers. Use of FPGA images intended for other product will render your chassis inoperable.

You can upgrade all Interface Module FPGA images through one procedure.

To upgrade LP FPGA images on all Interface modules using a single command, do the following:

1. Place the bundled FPGA image on a TFTP server to which the router has access, or on a PCMCIA flash card inserted in slot 1 or 2.
2. Copy the bundled image from the TFTP server or a flash card to all or specific interface modules. To perform this step, enter the following commands at the Privileged EXEC level of the CLI:

   From a TFTP server:

   ```
   NetIron#copy tftp lp 10.10.10.10 lpfpga03900.bin fpga-all all
   ```

   Syntax: Syntax: copy tftp lp <IP addr> <file_name> fpga-all [<slot#> | all] [force -overwrite | <module_type>]

   From a PCMICA flash card inserted in slot 1:

   ```
   NetIron#copy slot1 lp lpfpga03900.bin fpga-all all
   ```

   Syntax: Syntax: copy [slot1| slot2] lp <source_file_name> fpga-all [<slot#> | all] [force -overwrite | <module_type>]

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

   The<slot#> variable specifies the slot #.

   The <module_type> variable specifies the Interface Module whose FPGA is to be upgraded, such as 1xoc192.

The FPGA versions being installed will be compared against those currently on the interface modules. If both FPGA images are identical, the download is aborted and a message is sent, for example:

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

If the **all** option is used, the software 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 will proceed with the download.

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

Upgrading the FPGA Images One Image at a Time

WARNING: You must use an FPGA images that is specified for the NetIron MLX Series or NetIron XMR Series routers. Use of FPGA images intended for other product will render your chassis inoperable.

To upgrade one or more FPGA images on an Ethernet Interface module, perform the following steps:

1. Place the new FPGA image(s) on a TFTP server to which the router has access or on a PCMCIA flash card inserted in slot 1 or 2.
2. Copy the PBIF image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (for example: NetIron#):
   - **copy tftp lp** <ip-addr> <image-name> **fpga-pbif all** [<module-type>] [force-overwrite]
   - **copy tftp lp** <ip-addr> <image-name> **fpga-pbif** <chassis-slot-number> [force-overwrite]
   - **copy slot1** | **slot2 lp** <image-name> **fpga-pbif all** [<module-type>] [force-overwrite]
   - **copy slot1** | **slot2 lp** <image-name> **fpga-pbif** <chassis-slot-number> [force-overwrite]

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

   The FPGA versions being installed is compared against those currently on the interface modules. If both FPGA images are identical, the download is aborted and the following warning message is sent:

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

   If the **all** option is used, the software 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 will proceed with the download.

   If the **force-overwrite** option is used, an identical image will be downloaded and the warning message will not be sent.

   NOTE: Use this command to upgrade the PBIFOC FPGA image to a POS interface module.

3. Copy the XPP image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI:
   - **copy tftp lp** <ip-addr> <image-name> **fpga-xpp all** [<module-type>]
   - **copy tftp lp** <ip-addr> <image-name> **fpga-xpp** <chassis-slot-number>
   - **copy slot1** | **slot2 lp** <image-name> **fpga-xpp all** [<module-type>]
   - **copy slot1** | **slot2 lp** <image-name> **fpga-xpp** <chassis-slot-number>

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

The FPGA versions being installed is compared against those currently on the interface modules. If both FPGA images are identical, the download is aborted and the following warning message is sent:

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

If the **all** option is used, the software 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 will proceed with the download.

If the **force-overwrite** option is used, an identical image will be downloaded and the warning message will not be sent.

NOTE: Use this command to upgrade the XPPOC FPGA image to a POS interface module.

4. Copy the XGMAC image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI:

   - **copy tftp lp** <ip-addr> <image-name> **fpga-xgmac all** [<module-type>]
   - **copy tftp lp** <ip-addr> <image-name> **fpga-xgmac** <chassis-slot-number>
   - **copy slot1 | slot2 lp** <image-name> **fpga-xgmac all** [<module-type>]
   - **copy slot1 | slot2 lp** <image-name> **fpga-xgmac** <chassis-slot-number>

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

   The FPGA versions being installed is compared against those currently on the interface modules. If both FPGA images are identical, the download is aborted and the following warning message is sent:

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

   If the **all** option is used, the software 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 will proceed with the download.

   If the **force-overwrite** option is used, an identical image will be downloaded and the warning message will not be sent.

5. Copy the STATS image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI:

   - **copy tftp lp** <ip-addr> <image-name> **fpga-stats all** [<module-type>]
   - **copy tftp lp** <ip-addr> <image-name> **fpga-stats** <chassis-slot-number>
   - **copy slot1 | slot2 lp** <image-name> **fpga-stats all** [<module-type>]
   - **copy slot1 | slot2 lp** <image-name> **fpga-stats** <chassis-slot-number>

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

   The FPGA versions being installed is compared against those currently on the interface modules. If both FPGA images are identical, the download is aborted and the following warning message is sent:

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

If the **all** option is used, the software 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 will proceed with the download.

If the **force-overwrite** option is used, an identical image will be downloaded and the warning message will not be sent.

NOTE: Use this command to upgrade the STATSOC FPGA image to a POS interface module.

6. Once the FPGA upgrade is complete, the new FPGA images will take effect at the next system reload. Alternately, you can make the FPGA image take effect on an Interface module without reloading the Management module, by power cycling the Interface module by either of the following two methods:
   - power off and power on the Interface module by first using the **power-off lp** <*slot*> command and then the **power-on lp** <*slot*> command.
   - pull out and then reinsert the Interface module.
7. Upon boot-up of the Interface Module, the FPGA Version Check utility is run to make sure that compatible versions of the FPGA images are installed on the router. Upon boot-up or when the show version command is typed, the following will be displayed.

   ```
   Valid PBIF Version = 3.14, Build Time = 12/17/2008 14:32:00
   Valid XPP Version = 5.22, Build Time = 8/6/2009 19:10:00
   Valid XGMAC Version = 0.12, Build Time = 11/10/2008 15:50:00
   ```

   Also, one of the following warnings will be displayed if there is a problem with your FPGA installation.

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

   If this warning message is displayed it indicates that you have an FPGA version mismatch, or one of the versions is not up-to-date.

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

   If this warning message is displayed it indicates that you haven't done a mandatory FPGA upgrade yet.

Rebooting the Management Module

After upgrading one or more software images on the management or interface modules, you must reboot the management module. After the management module reboots, it in turn 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:

- If you have a standby management module, the active management module compares the standby module's monitor, primary, and secondary images to its own. If you have updated these images on the active module, the active module automatically synchronizes the standby module's images with its own.
- If you copied the primary and/or secondary IronWare image to all interface modules using the **copy** command with the **all** keyword, the management module made a copy of the image and stored it in its code flash under the names lp-primary-0 or lp-secondary-0. By default, the system checks the interface modules' IronWare images, which reside in the code flash of the interface modules and the management module to make sure they are the same in both locations. (These IronWare images are stored on the management module only and are not run by the management or interface modules.) If the IronWare images on the interface and management modules are different, the system prompts you to do the following:

- If you want to update the IronWare images in the interface module's code flash with the images in the management module's code flash, enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.
- If you want to retain the IronWare images in the interface module's code flash, enter the **lp cont-boot no-sync <slot-number>** command at the Privileged EXEC prompt.

After the management module finishes booting, do the following:

1. Enter the **show module** command at any CLI level, and verify that the status of all interface modules is CARD_STATE_UP.
2. Enter the **show version** command at any CLI level, and verify that all management and interface modules are running the new software image version.

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

Hitless OS Upgrade

NOTE: The 04.1.00b patch release does *not* support hitless upgrade from Multi-Service IronWare release 04.1.00.

Using Hitless OS upgrade, you can upgrade the Multi-Service IronWare software without a loss of service or disruption in the following supported functions and protocols:

- All ports and links remain operational
- TOS-based QoS
- Layer-2 Switching
- Layer-2 Protocols:
  - MRP
  - STP
  - RSTP
- Routing Protocols:
  - OSPF
  - BGP
- Static IP Routes
- Layer-3 Forwarding
- GRE Tunnels
- ACLs – The following ACLs will continue to function but counters used by ACL accounting 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

The following features are *not* supported by hitless OS upgrade:

- 802.1s
- All MPLS Features
- IPv4 and IPv6 Multicast
- VLAN Translation
- Policy-based Routing
- FPGA upgrades are not supported
- IPv6 unicast
- VRRP and VRRP-E
- All VPN features
- Network management to the device:
    - SSH
    - Telnet
    - SNTP
    - HTTP/HTTPS
    - sFlow (LP only)
    - Ping
    - Traceroute
    - Syslog messages are cleared
    - SNMP
    - SNMP trap
    - DNS
    - DHCP
    - AAA
- VSRP
- POS

NOTE: Services listed as not supported may encounter disruptions during reset of the management and interface modules but will resume normal operation once the modules are back up and running.

Considerations when using the Feature

Consider the following when using this feature:

- You must have both active and standby management modules installed to use this feature.
- To avoid any disruptions of Layer-3 traffic to OSPF or BGP routes, the router must be configured with OSPF Graceful Restart and BGP Graceful Restart features. In addition, the device's OSPF neighbors must have OSPF Graceful Restart Helper enabled.
- The total time it takes for the hitless upgrade process to finish varies between approximately 1 and 10 minutes. This depends on the size of the MAC table, the number of OSPF and BGP neighbors and the size

of the routing table. Router configuration is unavailable during the entire hitless upgrade process. The message "**---SW Upgrade In Progress - Please Wait---**" is printed at the console when configuration is attempted. Operational command of the router is allowed during the upgrade process.

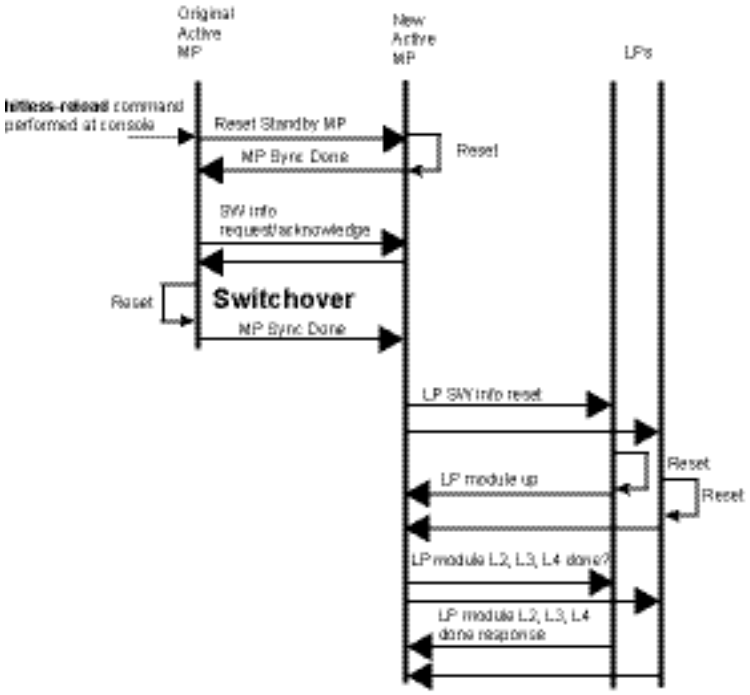
- The active management module changes from the initial active management module to the standby management module during the hitless upgrade process. This makes it necessary to have a connection to the console interface on both management modules.
- Upon being reset, the management and interface module CPUs are unable to send and receive any packets. Once the management and interface modules are up and running, their CPUs are able to send and receive packets, even before the Hitless Upgrade process is complete.
- Router configuration is not allowed to be changed during the entire 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 upon Hitless Upgrade.
- FPGA images cannot be upgraded using the Hitless Upgrade process.
- This feature cannot be used to downgrade an image to an older version than the version that the device is currently running.
- If there are protocol dependencies between neighboring nodes, Brocade recommends that you upgrade nodes one at a time.
- After hitless upgrade, the NetIron MLX or NetIron XMR router will still have the same running configuration as it does before the upgrade. A configuration that is not saved before hitless reload is not removed and the existing startup configuration does not take effect. This behavior is the same as displayed by the management module switchover feature.

The Hitless OS upgrade process

Hitless upgrade of Multi-Service IronWare software is performed in the following steps:

1. The Multi-Service IronWare software is installed in flash memory to the primary and secondary image on the active and standby management modules and interface modules.
2. Execute the **hitless-reload** command on the active management module.
3. The Hitless Upgrade process begins 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 assumes control as 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 operating on 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.

Figure 1 Management module (MP) and Interface Module (LP) Hitless Upgrade Process



Performing a Hitless OS software upgrade

To perform a Hitless OS software upgrade, you must perform the following tasks:

1. Copy the Multi-Service IronWare software to the primary and secondary image on both the active and standby management modules and interface modules.
2. Setup a console connection to both the active and standby management modules. These connections can be through a telnet, SSH, or serial console session.
3. Type the **hitless-reload** command at the console of the active management module.

Loading the Multi-Service IronWare software onto the Router

Hitless OS Upgrade loads from the primary and secondary images on the Management modules. The first step in performing a Hitless OS Upgrade is to copy the Version 03.2.01 or later images into the flash memory of the active and standby management modules.

For instructions for copying these files, see “Upgrading Monitor and Boot Images on a Management module” and “Upgrading the IronWare Image.”

Setting up Consoles

Hitless OS Upgrade is executed at the active management module. During the process of upgrading the image, control of the router shifts to the standby management module. For this reason, you need to have management sessions enabled on both the active and the standby management modules. When the reload is complete, the management module that was in the standby condition at the beginning will be in the active state. If you want the original management module to be active, you must manually fail-over control to it.

Executing the Hitless Upgrade Command

To begin the process of a Hitless Upgrade, use the following command:

```
NetIron(config)# hitless-reload mp primary lp primary
```

Syntax: **hitless-reload mp** [**primary | secondary**] | **lp** [**primary | secondary**]

The **mp** parameter specifies that the management module will be reloaded with either the **primary** or **secondary** image as directed.

The **lp** parameter specifies that the interface module will be reloaded with either the **primary** or **secondary** image as directed.

Software Image Coherence Check

The Multi-Service IronWare software has been enhanced to perform a verification process whenever the **reload-check** command is issued. This process checks to see that the router will be installing compatible versions of the operating software on the Management and Interface modules and also that all Interface module FPGAs are compatible with the application software image being loaded. 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

You can use 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... done.

Warning: The new MP application (3 6 0 13) will not be compatible with the new LP #
application (3 6 0 0) version

Warning: The new MP application (3 6 0 0) will not be compatible with the new LP #
application (3 5 0 0) version

Warning: The new LP application (3 6 0 13) on MP will not be compatible with the new
LP # application (3 6 0 0) version

Warning: The new LP monitor (3 6 0 0) on MP will not be compatible with the new LP
monitor (3 5 0 0) version

Warning: The new LP # application (3 6 0 0) will not be compatible with the new LP
monitor (3 5 0 0) version.

Warning: The new LP # application (3 6  0 0) will not be compatible with the new LP #
monitor (3 5 0 0) version.

Warning: The new LP PBIF FPGA will not be compatible with the new LP # application.

Warning: The new LP XPP FPGA will not be compatible with the new LP # application.

Warning: The new LP XPP XGMAC will not be compatible with the new LP # application.

Warning: The new LP PBIF-OC FPGA will not be compatible with the new LP # application.

Warning: The new LP XPP-OC FPGA will not be compatible with the new LP # application.

Warning: The new LP SPP STATS-OC will not be compatible with the new LP # application.

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

Syntax: **reload-check**

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: In situations where the Interface modules are in interactive mode, or the system is unable to communicate with the Interface modules, the system will send the following warning message: `Can't check LP for coherence`.

Image Files in Multi-Service IronWare Release 04.1.00b for the NetIron CER and NetIron CES Series

The following Software Image Files are available for Multi-Service IronWare release 04.1.00b for the NetIron CES 2000 series and NetIron CER 2000 series switches.

Image File Names		
Image Type	**Function**	**Image Name**
Boot	Bootstrap	ceb04100a.bin
Monitor	Image Handling Memory Init	ceb04100b.bin
Multi-Service IronWare	Application OS	ce04100b.bin

NOTE: The NetIron CES 2000 series and NetIron CER 2000 series use the same file image for both the boot and monitor images.

Upgrading Software on the NetIron CER and NetIron CES Series

Images and Procedures Required

NOTE: Throughout the sections below, procedures described for the NetIron CES 2000 Series switch are also applicable to the NetIron CER 2000 Series switch except where indicated.

The software images required and the procedures for upgrading are described in the following sections:

- Upgrading the Multi-Service IronWare Software – This sub-section describes the procedures required for your software upgrade.
- Displaying the Flash Memory and Version Information – This sub-section describes the commands that allow you to determine the contents of the NetIron CES 2000 Series switch's flash memory and how to read the output of those commands.
- Upgrading the Device's Monitor and Boot Images – This sub-section describes the procedures required for upgrading the NetIron CES 2000 Series Switches Monitor and Boot software images. The procedures described apply to all versions of the software.
- Upgrading the Device's Multi-Service IronWare Image – This sub-section describes the procedures required for upgrading the NetIron CES 2000 Series Switches Multi-Service IronWare software image. The procedures described apply to all versions of the software.
- Rebooting the Device – This sub-section describes the procedures required for rebooting the device after upgrading the software images.

Upgrading the Multi-Service IronWare Software

When performing this upgrade, you will usually only need to upgrade Multi-Service IronWare image. The Boot and Monitor images will only need to be upgraded as specifically directed in the relevant release notes.

The steps for this upgrade include the following:

1. Determine the versions of the software images currently installed and running on the switch.
2. Upgrade the Multi-Service IronWare Image.
3. Reboot the NetIron CES 2000 Series switch.

In most cases, this is all that will be required. If you are directed by the release notes to upgrade the Monitor or Boot images, use the following procedures:

1. Upgrade the NetIron CES 2000 Series switches Monitor and Boot images.

   Use the procedures described in “Upgrading the Device’s Monitor and Boot Images .”

2. Reboot the NetIron CES 2000 Series Switch.

Displaying Flash Memory and Version Information

Prior to upgrading the images on a NetIron CES 2000 Series switch, it is advisable to check the versions already installed. This allows you to determine which versions need to be upgraded. It is also useful to check the versions installed immediately after an upgrade has been done to make sure that you have installed the versions required in your installation. The following sections describe how to use the **show flash** and **show version** commands to display this information.

Displaying flash Information

You can display information concerning the contents of a NetIron CES 2000 Series switch using the **show flash** command as shown in the following:

```
NetIron CES#show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Code Flash - Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 4.1.0bT183, Size 7848114 bytes, Check Sum 361a
    Compiled on Mar 10 2010 at 15:54:18 labeled as ce04100b
  o Monitor Image
    Version 4.1.0bT185, Size 361779 bytes, Check Sum 4f78
    Compiled on Mar 10 2010 at 15:22:34 labeled as ceb04100b
  o Startup Configuration
    Size 1372 bytes, Check Sum c163
    Modified on 22:55:34 GMT+00 Tue Jan 09 2001

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 4.1.0T185, Size 360882 bytes, Check Sum 4c37
    Compiled on Sep  4 2009 at 13:34:24 labeled as ceb04100b135
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
NetIron CES#
```

Likewise, you can display information concerning the contents of a NetIron CER 2000 Series switch using the **show flash** command as shown in the following:

```
NetIron CER#show flash
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Code Flash - Type MT28F128J3, Size 32 MB
  o IronWare Image (Primary)
    Version 4.1.0bT183, Size 7848114 bytes, Check Sum 361a
    Compiled on Mar 10 2010 at 15:54:18 labeled as ce04100b
  o Monitor Image
    Version 4.1.0bT185, Size 361779 bytes, Check Sum 4f78
    Compiled on Mar 10 2010 at 15:22:34 labeled as ceb04100b
  o Startup Configuration
    Size 1372 bytes, Check Sum c163
    Modified on 22:55:34 GMT+00 Tue Jan 09 2001

Boot Flash - Type AM29LV040B, Size 512 KB
  o Boot Image
    Version 4.1.0T185, Size 360882 bytes, Check Sum 4c37
    Compiled on Sep  4 2009 at 13:34:24 labeled as ceb04100b135
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
NetIron CER#
```

Syntax: **show flash**

Code flash and boot flash information	
This Field...	**Displays...**
Code Flash	The model number and size of the NetIron CES 2000 Series Switches code flash.
Multi-Service IronWare Image (Primary or Secondary)	Indicates the Multi-Service IronWare image installed in the primary or secondary location in the NetIron CES 2000 Series Switches code flash. The image must be ce <xxxxx>. The actual image name depends on the version of software you have running on your switch. The output displays the following information about the image: • Version – " 3.9.0Txxy" indicates the image version number. The "Txxy" is used for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that Brocade compiled the image.
Monitor Image	The image must be ceb<xxxxx>. The output displays the following information about the image: • Version – " 3.9.0Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that Brocade compiled the image.
Startup Configuration	The output displays the following information about the startup configuration: • Size – Size, in bytes, of the startup configuration. • Check sum – A unique ID for the file. If the contents of the file change, the check sum changes also. • Modification date and time – Date and time that the startup configuration was last saved.
Boot Flash	The model number and size of the device's boot flash.
Boot Image	The image must be ceb <xxxxx>. The output displays the following information about the image: • Version – " 3.9.0Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Check sum – A unique ID for the image. If the contents of the image change, the check sum changes also. • Compilation date and time – The date and time that Brocade compiled the image.

Displaying Version Information

You can display version information for a NetIron CES 2000 Series switch using the **show version** command.

```
NetIron CES#show version
HW: NetIron CES ALLSW_PREM
System (Serial #: SA18091365,  Part #: 36001-002B)
Boot     : Version 4.1.0aT185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jan  5 2010 at 19:44:32 labeled as ceb04100a
 (357766 bytes) from boot flash
Monitor  : Version 4.1.0bT185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 10 2010 at 15:22:34 labeled as ceb04100b
 (361779 bytes) from code flash
IronWare : Version 4.1.0bT183 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 10 2010 at 15:54:18 labeled as ce04100b
 (7848114 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000c
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
512 MB DRAM
System uptime is 12 seconds
NetIron CES#
```

Likewise, you can display version information for a NetIron CER 2000 Series switch using the **show version** command.

```
NetIron CER#show version
HW: NetIron CER ADV_SVCS_PREM
System (Serial #: SA18091365,  Part #: 36001-002B)
Boot     : Version 4.1.0aT185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Jan  5 2010 at 19:44:32 labeled as ceb04100a
 (357766 bytes) from boot flash
Monitor  : Version 4.1.0bT185 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 10 2010 at 15:22:34 labeled as ceb04100b
 (361779 bytes) from code flash
IronWare : Version 4.1.0bT183 Copyright (c) 1996-2009 Brocade Communications Systems,
Inc.
Compiled on Mar 10 2010 at 15:54:18 labeled as ce04100b
 (7848114 bytes) from Primary
CPLD Version: 0x00000010
Micro-Controller Version: 0x0000000c
800 MHz Power PC processor 8544 (version 8021/0022) 400 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
512 MB DRAM
System uptime is 12 seconds
NetIron CER#
```

Syntax: **show version**

The highlighted lines in the output indicate the versions currently running boot, monitor and Multi-Service IronWare images for the NetIron CES 2000 Series Switches. The fields are described in Table 4 except for the following:

The "HW:" line indicates the hardware ("NetIron CES") and the type of software package enabled on the unit. The type of software package enabled on the system can be one of the following:

- BASE: Indicates that the BASE software package is enabled on the unit.
- ME_PREM: Indicates that the ME_PREM premium package is enabled on the unit.

- L3_PREM: Indicates that the L3_PREM premium package is enabled on the unit.

For a detailed description of the features available in each type of software package, please refer to the *NetIron Series Configuration Guide*.

Backing Up the Current Software Images

Before performing a software upgrade, Brocade recommends backing up the following current software images in the device's flash memory.

Syntax: **cp** <*original-file-name*> <*backup-file-name*>

Upgrading the Device's Monitor and Boot Images

If you are upgrading, you should only upgrade the monitor and boot images as described in the relevant release notes.

To upgrade a device's monitor and boot images, perform the following steps:

1. Place the new monitor and boot images on a TFTP server to which the switch has access.
2. Copy the new monitor and boot images to the switch. Enter one of the following commands at the Privileged EXEC level of the device's CLI (example: NetIron#):

Command syntax for upgrading monitor and boot images on the NetIron CES and NetIron CER series switches	
Command Syntax	**Description**
copy tftp flash <ip-addr> <image-name> **monitor**	Copies the latest monitor image from the TFTP server to flash.
copy tftp flash <ip-addr> <image-name> **boot**	Copies the latest boot image from the TFTP server to flash.

   For information about the image name to specify, see Software Image Files for Multi-Service IronWare Release 04.1.0.

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*>/

   Check for the boot image, monitor image, and the date and time at which the new images were built.
4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the switch to complete the upgrade process.

Upgrading the NetIron CES and NetIron CER series Switch's Multi-Service IronWare Image

To upgrade the NetIron CES or NetIron CER series switch's Multi-Service IronWare image (primary or secondary), you must perform the following steps:

1. Copy the new Multi-Service IronWare image from the TFTP server to the code flash. To perform this step, enter the following command at the Privileged EXEC level of the CLI:

copy tftp flash <*ip-addr*> <*image-name*> **primary | secondary**

For information about the image name to specify, see Software Image Files for Multi-Service IronWare Release 04.1.0

2. Verify that the new Multi-Service IronWare 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*>/

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

3. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the device to complete the upgrade process.

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 the management module's 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 2000 Series Switches 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 NetIron 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 allows you to specify the configuration file size you want for processing various commands.

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

NOTE: Brocade strongly recommends using the default size (8MB) when configuring file size.

After you issue the system-max command, with the config-file-size parameter included, additional information following will display:

```
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 write this command to memory and perform a system reload 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 those changes by writing them to code flash. When you write configuration changes to code flash, you replace the startup configuration with the running configuration.

To replace the startup configuration with the running configuration, enter the following command at any Enable or CONFIG command prompt:

```
NetIron # write memory
```

Replacing the Running Configuration with the Startup Configuration

If you haven't yet executed a write memory command to overwrite the startup configuration with the running configuration and you want to back out of the changes you have made to the running configuration and return to the startup configuration, enter the following command at the Privileged EXEC level of the CLI:

```
NetIron# reload
```

When 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 NetIron MLX Series router, the file is always copied as "startup-config" or "running-config", depending on which type of file you saved to the server.

To initiate transfers of configuration files to or from a TFTP server, enter one of the following commands at the Privileged EXEC level of the CLI:

- **copy startup-config tftp** <*tftp-ip-addr*> <*filename*> – Use this command to upload a copy of startup-config from the NetIron router to a TFTP server.
- **copy running-config tftp** <*tftp-ip-addr*> <*filename*> – Use this command to upload a copy of the running configuration from the NetIron router to a TFTP server.
- **copy tftp startup-config** <*tftp-ip-addr*> <*filename*> – Use this command to download a copy of the startup-config from a TFTP server to the NetIron router.

- **copy tftp running-config** <*tftp-ip-addr*> <*filename*> [**overwrite**] – Use this command to download the running configuration from the system's runtime memory to a TFTP server. The running configuration is then appended to the current configuration of the NetIron router.

Making Local Copies of the Startup Configuration File

You can copy the startup-config file in code flash to a TFTP server or to a PCMCIA flash card inserted in a Management Module's 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 if you want 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.

Technical Support

Contact your switch 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
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
2. **Switch 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

Go to kp.foundrynet.com and log in to the Knowledge Portal (KP) to obtain more information about a product, or to report documentation errors. To report errors, click on Cases > Create a New Ticket. Make sure you specify the document title in the ticket description.

Email Access

Send an e-mail to support@foundrynet.com

Telephone Access

United States: 1.800.752.8061 United States

Europe and Africa (not toll free) +1 800-AT-FIBREE (+1 800 28 34 27 33)

Asia Pacific (not toll free) +1 800-AT FIBREE (+1 800 28 34 27 33)

Areas unable to access 800 numbers: +1 408.333.6061

Additional Resources

Below are some additional publications you can reference to find more information on the products supported in this software release.

Title	Contents

Hardware Installation Guide for the NetIron CES 2000 Series	• Product Overview
	• Installation
	• Basic Configuration
	• Hardware Maintenance and Replacement
	  ◦ Fiber optic connectors
	  ◦ Replaceable modules
	  ◦ AC Power supply
	  ◦ Fans
	• Software Upgrades
	• Hardware Specifications
	• Regulatory Statements

NetIron Series 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.

Title	Contents

Brocade *NetIron MLX Series Installation and Basic Configuration 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

Brocade *NetIron XMR Series Installation and Basic Configuration 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 Series Configuration Guide	Contains all configuration information for the NetIron XMR and NetIron MLX Series of routers.
IronWare MIB Guide	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
NetIron XMR and MLX Diagnostic Reference	This manual describes troubleshooting and diagnostic commands available in the IronWare command line interface (CLI) for NetIron XMR and MLX routing devices.
Brocade IronView Network Management User's Guide	SNMP-based application for managing Brocade switches and switching routers.

Documentation Updates

This section presents last minute additions to the NetIron Series Configuration Guide. The latest issue of the guide is available on the Brocade Knowledge Portal at kp.foundrynet.com.

Setting IPv6 Default Router Preference

Starting with release 4.1.00, by default the NetIron uses a fixed value of "medium" for the default router preference in IPv6 neighbor discovery router advertisement. Patch release 04.1.00b provides a new CLI command which allows you to change the default router preference value.

To set the default router preference, enter commands similar to the following.

```
NetIron(config)# interface ethernet 3/1
NetIron(config-if-e100-3/1)# ipv6 nd router-preference high
```

Syntax: [**no**] **ipv6 nd router-preference** <**high** | **medium** | **low**>

When router life time is not zero, the next router advertisement message sent out from this interface will use a Default Router Preference (DRP) as configured using the above command. If router life time is zero, regardless of the value configured using the above command, the next router advertisement message sent out from this interface will use a DRP value of medium.

Defects

Closed Defects Affecting One or Both Platforms R04.1.00b

Defect ID: DEFECT000104833	**Technical Severity:** High
Summary: A Management Module may reload while processing IGMP packet with non-zero padding that is received on port that is not multicast enabled.	
Probability: Medium	
Feature: IP Forwarding	**Function:** IP Forwarding
Reported In Release: NI 04.1.00	**Service Request ID:** 226763

Defect ID: DEFECT000109870	**Technical Severity:** High
Summary: A Management Module can sometimes reload unexpectedly on NetIron XMR or NetIron MLX devices that are configured with Exec Accounting and System Accounting.	
Probability: Low	
Feature: Security	**Function:** AAA
Reported In Release: NI 04.1.00	**Service Request ID:** 235910

Defect ID: DEFECT000110279	**Technical Severity:** Low
Summary: With multiple, simultaneous telnet sessions accessing CLI, the reload command from one of the sessions does not take effect.	
Probability: Low	
Feature: System	**Function:** CLI
Reported In Release: NI 04.1.00	**Service Request ID:** 235910

Defect ID: DEFECT000110543	**Technical Severity:** Medium
Summary: OSPF P2P does not send a SNMP trap on an interface UP event.	
Probability: High	
Feature: OSPF, SNMP Management	**Function:** SNMP Logging
Reported In Release: NI 04.1.00	**Service Request ID:** 236174

Defect ID: DEFECT000274283	**Technical Severity:** Medium
Summary: A device connected to two SVLAN ports may fail to communicate if the SVLAN is a member of ISID.	
Probability: Medium	
Feature: CES 802.1ad	**Function:** Forwarding
Reported In Release: NI 04.1.00	**Service Request ID:** 237743

Defect ID: DEFECT000274789	**Technical Severity:** Medium
Summary: Warning message for the command "no router ospf vrf <name>" is misleading.	
Probability: Medium	
Feature: OSPF	**Function:** CONFIGURATION
Reported In Release: NI 04.1.00	**Service Request ID:** 239102

Defect ID: DEFECT000275817	**Technical Severity:** Medium
Summary: Configuring "cam-mode ip dynamic" and "ip net-aggregate" may cause unexpected reboot of LP modules	
Probability: High	
Feature: CES IPv4 Forwarding	**Function:** Routing
Reported In Release: NI 04.1.00	**Service Request ID:** 238233

Defect ID: DEFECT000275880	**Technical Severity:** High
Summary: When loading sbridge image from a system running 4.1.00, the image on the SFMs may get corrupted.	
Workaround: Do not update the sbridge image as there is NO need.	
Probability: High	
Feature: System - XMR/MLX	**Function:** SFM
Reported In Release: NI 04.1.00	**Service Request ID:** 238866

Defect ID: DEFECT000276836	**Technical Severity:** Medium
Summary: "no" (delete) commands do not work when copying config file from tftp to running via snmpset	
Risk of Fix: Medium	
Feature: TFTP	**Function:** CLI
Reported In Release: NI 04.0.00	**Service Request ID:** 219974

Defect ID: DEFECT000277165	**Technical Severity:** Medium
Summary: when "route-only" is configured on individual ports, the port keeps forwarding the known L2 unicast packet.	
Probability: Medium	
Feature: L2 Forwarding - XMR/MLX	**Function:** Forwarding
Reported In Release: NI 04.1.00	**Service Request ID:** 238690

Defect ID: DEFECT000277167	**Technical Severity:** Medium
Summary: When booting, MP cannot load image from PCMCIA slot1 or slot2.	
Risk of Fix: Low	
Feature: System - XMR/MLX	**Function:** Flash memory
Reported In Release: NI 04.0.00	**Service Request ID:** 237247

Defect ID: DEFECT000278289	**Technical Severity:** High
Summary: Issuing the command 'show cam violation 0' may cause the system to reload unexpectedly.	
Workaround: Do not issue this command.	
Probability: Low	**Risk of Fix:** Low
Feature: System - XMR/MLX	**Function:** TCAM programming
Reported In Release: NI 03.9.00	**Service Request ID:** 240288

Defect ID: DEFECT000279176	**Technical Severity:** Medium
Summary: LP may reload unexpectedly when it receives an IPv6 sFlow packet on a VRF interface and IPv6 is not configured for the VRF.	
Probability: Medium	
Feature: IPV6	**Function:** RTM
Reported In Release: NI 04.1.00	**Service Request ID:** 240324

Defect ID: DEFECT000279178	**Technical Severity:** Critical
Summary: With IP multicast traffic running, disabling PIM, may cause the system to reload unexpectedly.	
Feature: IPv4-MC PIM-SM Routing	**Function:** PROTOCOL
Reported In Release: NI 04.1.00	**Service Request ID:** 241003

Defect ID: DEFECT000279319	**Technical Severity:** Medium
Summary: System does not allow to configure port name with more than 32 characters.	
Feature: CLI Infrastructure	**Function:** Parser Engine
Reported In Release: NI 04.1.00	**Service Request ID:** 240601

Defect ID: DEFECT000279442	**Technical Severity:** High
Summary: CLI does not enforce max number of per-packet trunk type limit of 4 when configuring static LAG.	
Probability: High	**Risk of Fix:** Low
Feature: LAG - XMR/MLX	**Function:** Static
Reported In Release: NI 04.0.00	**Service Request ID:** 240538

Defect ID: DEFECT000279955	**Technical Severity:** Medium
Summary: IPv6 Traps are not sent if an IPv4 address is not configured on the XMR/MLX or RX.	
Probability: Medium	**Risk of Fix:** Medium
Feature: SNMP Management	**Function:** Trap/Notification
Reported In Release: NI 04.0.00	**Service Request ID:** 241172

Defect ID: DEFECT000280060	**Technical Severity:** High
Summary: Stale M'cast state remain on the MP & LP after the source has long since stopped sending Stream.	
Probability: High	**Risk of Fix:** High
Feature: IPv4-MC PIM-SM Routing	**Function:** PERFORMANCE
Reported In Release: NI CES 03.9.00	**Service Request ID:** Tony Ho

Defect ID: DEFECT000280248	**Technical Severity:** Medium
Summary: Sflow packets have incorrect source-id field which results in InMon not processing these packets.	
Probability: Medium	
Feature: Sflow - XMR/MLX	**Function:** General
Reported In Release: NI 04.1.00	**Service Request ID:** 241305

Defect ID: DEFECT000280767	**Technical Severity:** Medium
Summary: Router discards pim registration stop messages if it is received on non-pim-enabled interface.	
Probability: Medium	**Risk of Fix:** Low
Feature: IPv6-MC PIM-SM Routing	**Function:** Concurrent Routing/Snooping
Reported In Release: NI 04.0.00	**Service Request ID:** 240996

Defect ID: DEFECT000280898	**Technical Severity:** Medium
Summary: Aborting a trace-l2 command on a vlan and then issuing a follow-on “trace-l2 show” command may cause the system to reload unexpectedly.	
Probability: Medium	**Risk of Fix:** Low
Feature: Traceroute	**Function:** PROTOCOL
Reported In Release: NI 03.9.00	**Service Request ID:** 241685

Defect ID: DEFECT000281084	**Technical Severity:** Medium
Summary: MAC ACL name with special character "/" is not handled correctly.	
Probability: Medium	
Feature: ACL - XMR/MLX	**Function:** L2 ACL
Reported In Release: NI 04.1.00	**Service Request ID:** 241798

Defect ID: DEFECT000281227	**Technical Severity:** Medium
Summary: MLX system limit of 262144 maximum ip-vrf-routes is not enforced by CLI.	

Probability: High	
Feature: IPv4	**Function:** CONFIGURATION
Reported In Release: NI 04.1.00	**Service Request ID:** 241532

Defect ID: DEFECT000282187	**Technical Severity:** Medium
Summary: Copying large ACL to running config can cause VRRP-e to flap	
Probability: Medium	**Risk of Fix:** Medium
Feature: ACL - XMR/MLX	**Function:** IPv4 ACL
Reported In Release: NI 03.8.00	**Service Request ID:** 240179

Defect ID: DEFECT000283294	**Technical Severity:** Medium
Summary: When traffic engineering policy is not configured for a specific area, then OSPF sends the topology update only in area 0 instead of the area configured on the device.	
Workaround: Work around is to configure area id with traffic-eng ospf. traffic-eng ospf area <area-id>	
Probability: Medium	
Feature: MPLS Control Plane	**Function:** CSPF
Reported In Release: NI 04.1.00	**Service Request ID:** 242678

Defect ID: DEFECT000285100	**Technical Severity:** Medium
Summary: "show memory" command does not display correct value for the diff between malloc and free counters.	
Risk of Fix: Low	
Feature: System - XMR/MLX	**Function:** Flash memory
Reported In Release: NI 04.0.00	**Service Request ID:** 243391

Defect ID: DEFECT000285232	**Technical Severity:** Medium
Summary: XMR and MLX systems should display maximum System-max ip-vrf-route value of 262144.	
Feature: VRF	**Function:** CLI
Reported In Release: NI 04.1.00	**Service Request ID:** 241532

Defect ID: DEFECT000285475	**Technical Severity:** Medium
Summary: L3VPN traceroute may miss one entry when source node is reachable through a default route.	
Probability: Medium	**Risk of Fix:** Medium
Feature: MPLS Forwarding - XMR/MLX	**Function:** L3VPN 2547
Reported In Release: NI 04.0.00	**Service Request ID:** 243676

Defect ID: DEFECT000287388	**Technical Severity:** High
Summary: When an IP multicast receiver leaves or joins a group, L2 Multicast stream for VPLS endpoints may experience some loss, while HW entries are reprogrammed.	
Probability: High	**Risk of Fix:** Medium
Feature: IPv4-MC Snooping- VPLS	**Function:** Resource Sharing/Forwarding
Reported In Release: NI 04.0.00	**Service Request ID:** 239610

Defect ID: DEFECT000287918	**Technical Severity:** High
Summary: When a RP receives a copy of an SA from more than one MSDP peers, system may not prevent looping properly.	
Feature: IPv4-MC MSDP	**Function:** PROTOCOL
Reported In Release: NI 04.1.00	**Service Request ID:** 235817

Defect ID: DEFECT000274267	**Technical Severity:** Medium
Summary: LSP uptime can be easily rolled over due to the time unit is in milliseconds.	
Feature: MPLS Control Plane	**Function:** LSP Manager
Reported In Release: NI 04.1.00	**Service Request ID:** 236868

Closed with Code Change Defects Affecting Both Platforms R04.1.00

Defect ID	Technical Severity	Closed with Code Change Defects Affecting Both Platforms R04.1.00
79319	High	**Summary:** Route change events may unnecessarily cause short disruptions for PIM traffic. **Probability:** High **Feature:** PIM Sparse **Function:** PIM Sparse **Reported in Release:** NetIron XMR and NetIron MLX R03.8.00
83734	High	**Summary:** ISIS configured with **redistribute connected** does not remove a redistributed connected route when ISIS is then configured on that interface. **Probability:** High **Feature:** ISIS **Function:** ISIS **Reported in Release:** NetIron XMR and NetIron MLX R03.7.00d
84023	High	**Summary:** Entering the command **snmp-server view statistics ifXTable included** causes system reboot. **Probability:** High **Feature:** SNMP **Function:** SNMP **Reported in Release:** NetIron XMR and NetIron MLX R03.8.00
88375	High	**Summary:** ISIS may experience "ISIS: Memory Limit Exceeded" errors under persistent route flapping. **Probability:** High **Feature:** ISIS **Function:** ISIS **Reported in Release:** NetIron XMR and NetIron MLX R03.7.00d
92029	Medium	**Summary:** Inconsistent TFTP error messages are displayed when TFTP times out. **Probability:** Medium **Feature:** TFTP **Function:** TFTP **Reported in Release:** NetIron XMR and NetIron MLX R03.8.00b
103682	High	**Summary:** MRP interfaces get stuck in forwarding when configured on the master VLAN of a topology group after a member VLAN is added to the topology group. **Probability:** High **Feature:** MRP, Topology Groups **Function:** MRP, Topology Groups **Reported in Release:** RX R02.6.00g
105464	High	**Summary:** Under rare conditions, CPU utilization profiling could cause a device to reset. **Probability:** Medium **Feature:** System **Function:** System **Reported in Release:** RX R02.5.00d

Defect ID	Technical Severity	Closed with Code Change Defects Affecting Both Platforms R04.1.00
106494	High	**Summary:** Under certain circumstances, PIM could corrupt its neighbor list causing the multicast task to reset. **Probability:** Medium **Feature:** PIM **Function:** PIM **Reported in Release:** CES R03.8.00e
109501	High	**Summary:** After repeatedly flapping the port intended for MPLS LSP primary path in FRR configuration, some LSPs may stay with their secondary path even after the port is restored. **Probability:** Medium **Feature:** MPLS **Function:** MPLS FRR **Reported in Release:** NetIron XMR and NetIron MLX R04.0.00d

Open Defects Affecting Both Platforms R04.1.00

Defect ID	Technical Severity	Open Defects Affecting Both Platforms R04.1.00
91084	Medium	**Summary:** PIM receiver on same VLAN as the LAG to the source router may fail to receive traffic for a few minutes when it joins again. **Probability:** Low **Feature:** PIM Dense; LAG **Function:** PIM Dense **Reported in Release:** NetIron CES R03.8.00
107808	Medium	**Summary:** For a BGP aggregate route, when both the as-set option and the attribute-map route-map option with the set as-path prepend setting are configured, the prepended as-path value appears twice in the final as-path of the aggregated route. **Workaround:** Set the complete as-path via the attribute-map. This can be configured on Neighbor outbound route-map. **Probability:** Medium **Feature:** BGP **Function:** BGP Route Map **Reported in Release:** NetIron XMR and NetIron CES R04.1.00
109306	High	**Summary:** OSPF opaque LSAs are not advertised for MPLS interfaces if **router mpls** and traffic-engineering policies are configured before **router ospf** is configured. **Workaround:** Configure **router ospf** first, then configure **router mpls** and **TE-policy**. **Probability:** Medium **Feature:** MPLS, OSPF **Function:** MPLS Traffic Engineering **Reported in Release:** NetIron MLX, NetIron XMR, NetIron CES and NetIron CER R04.1.00

Defects Affecting the NetIron XMR and NetIron MLX Series

Closed with Code Change Defects in the NetIron XMR and NetIron MLX Series R04.1.00

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
93279	Low	**Summary:** Remove incorrect reference in help string to the undebug command, which does not exist. **Probability:** High **Feature:** Debug **Function:** CLI
97045	High	**Summary:** Port security may continue to enforce a deny MAC address even after the configuration is removed, under some configuration change scenarios. **Probability:** Medium **Feature:** Port Security **Function:** Port Security Deny Mac list
99034	Low	**Summary:** A disabled 1GE fiber port without SFP inserted may occasionally report flapping. **Probability:** Low **Feature:** Optics **Function:** Link Status
99096	High	**Summary:** Upon hitless upgrade, messages about ITC errors appear on a Management Module console. **Probability:** Medium **Feature:** Hitless upgrade **Function:** Hitless upgrade
99464	High	**Summary:** In some occasions, LDP deletion of FEC is not handled properly leading to observed mismatch of labels between peers after an IGP route flap event. **Probability:** Medium **Feature:** MPLS **Function:** LDP **Workaround:** Clear the LDP neighbor.
99996	Medium	**Summary:** If a VPLS VLAN port has mac access-group enable-deny-logging configured, the removal of such a port to return to the default VLAN would fail. **Probability:** High **Feature:** VPLS **Function:** L2 ACL
100434	High	**Summary:** VPLS CPU forwarded packets are incorrectly dropped if the qos trust dscp command is configured on the MPLS interface. **Probability:** High **Feature:** MPLS **Function:** VPLS **Workaround:** Use the qos dscp decode-map command instead of the qos trust dscp command.
100717	Medium	**Summary:** In VLAN scaling situation, information about some VLANs may fail to reach line cards, impacting operations such as ARP resolution. **Probability:** Low **Feature:** VLAN **Function:** VLAN

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
100740	Medium	**Summary:** Outbound mirroring does not work for CPU forwarded packets. **Probability:** High **Feature:** Mirroring **Function:** Outbound Mirroring **Workaround:** Disable & enable the monitored port.
100763	Medium	**Summary:** VPLS instance configuration with dual mode endpoint may be incorrect, when the configuration is done by cut & paste on a telnet session. **Probability:** Medium **Feature:** VPLS **Function:** CLI **Workaround:** Please use CLI mode for this configuration.
101228	Medium	**Summary:** For ECMP routes with some next-hops over LAGs, flapping of some port of a LAG would lead to reprogramming of the ECMP PRAM unnecessarily, even though the LAG still has other working ports. **Probability:** High **Feature:** ECMP **Function:** IP Load-sharing
101509	High	**Summary:** A Management CPU may reload unexpectedly if a telnet session is disconnected, while an image copying through the telnet session is still in progress. **Probability:** Low **Feature:** Management **Function:** TFTP
101565	High	**Summary:** During RSVP LSP failover, a router fails to send RESV_TEAR message. **Probability:** High **Feature:** MPLS **Function:** RSVP
101646	High	**Summary:** An mplsLspTable entry may show two rows if a RSVP LSP is using secondary path as the active path. **Probability:** High **Feature:** MPLS **Function:** SNMP Mib
101677	Medium	**Summary:** OSPF summarized route cost is not compliant with RFC1583 even though rfc1583-compatibility command is configured. **Probability:** High **Feature:** IP Protocol **Function:** OSPF
102032	High	**Summary:** VPLS may incorrectly learn a broadcast SA in a MAC table and create a CAM entry, leading to subsequent packets with such broadcast DA to be dropped. **Probability:** High **Feature:** MPLS **Function:** VPLS
102072	High	**Summary:** Pending ARP entries are not deleted and may fill up the ARP table. **Feature:** IP Forwarding **Function:** ARP

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
102187	High	**Summary:** If a Layer 3 VPN packet in the direction of PE to CE is CPU forwarded, the router fails to properly remove its MPLS header. **Probability:** High **Feature:** MPLS **Function:** L3 VPN
102254	High	**Summary:** BGP peering connections that have been up continuously for over a year can flap down and up spontaneously. **Probability:** High **Feature:** IP Protocol **Function:** BGP
102289	High	**Summary:** A Management Module may reload unexpectedly during configuration change for RSVP LSP select-path command. **Probability:** Medium **Feature:** MPLS **Function:** LSP Select-path
102477	Low	**Summary:** Pager buffer overrun occurs when issuing the show span root command with 2000+ VLANs. **Probability:** High **Feature:** Root protect **Function:** CLI
102498	High	**Summary:** A Management Module may reload unexpectedly when the multicast RP table size grows, and causes internal message buffer corruptions. **Probability:** Low **Feature:** IP Multicast **Function:** PIM-Sparse **Workaround:** Disable BSR on the router or limit the number of RP-set.
102533	High	**Summary:** In some cases MSTP port with root-protect stays in an Inconsistent state for 300 seconds. **Probability:** High **Feature:** L2 Protocols **Function:** Root Protect
102534	Medium	**Summary:** When creating multiple trunks simultaneously through multiple telnet sessions, executing deploy within one affects the commands available within all. **Probability:** Medium **Feature:** LAG **Function:** CLI
102535	Low	**Summary:** The output from the show sflow command does not properly display the Actual default sampling rate. **Probability:** High **Feature:** Sflow **Function:** CLI
102573	High	**Summary:** For VLANs configured in 802.1s MSTP, the ports which are not part of the first VLAN in the vlan-range of a MSTP instance will not send or receive traffic. **Probability:** Medium **Feature:** MSTP **Function:** MSTP

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
102577	High	**Summary:** ServerIron sync packets (etye 885a) are not forwarded when UDLD is configured on some of the ports of the same PPCR. **Probability:** High **Feature:** UDLD **Function:** UDLD
102782	Medium	**Summary:** In some cases, ISIS interface shows UP even if ipv6 unicast-routing is not enabled. **Probability:** High **Feature:** IP Protocol **Function:** IS-IS
102856	Medium	**Summary:** On the system with FDP configured, ports on a newly hot inserted line card do not get added to the control VLAN needed for FDP. **Probability:** Low **Feature:** Management **Function:** FDP
102915	High	**Summary:** When link-error-disable with toggle value of 1 is configured on an interface, it could be erroneously triggered when its module is powered off and then powered on. **Probability:** Medium **Feature:** Port Flap Dampening **Function:** link-error-disable toggle threshold **Workaround:** Use toggle threshold value of 2 or more.
102927	High	**Summary:** An 802.1q tag in a STP BPDU may be stripped off at a VLL egress port with non-8100 tag-type, if spanning tree is enabled. **Probability:** High **Feature:** MPLS **Function:** VLL
102940	Medium	**Summary:** Some power supplies on a NetIron XMR-32 or NetIron MLX-32 chassis may be inaccessible after manually powering them off and on via the CLI. **Probability:** Medium **Feature:** Management **Function:** Power Supply **Workaround:** User should wait for 30 seconds before turning on the power supply via the CLI. If the power supply is in an inaccessible state, then reseat the power supply or reboot the router.
102953	Low	**Summary:** After a module is shut down due to exceeding shut-down temperature, the syslog message about the module powered off may be generated more than once. **Probability:** High **Feature:** Management **Function:** Syslog
103113	High	**Summary:** Upon link-up, link-error-disable assessment should be made first before LAG threshold recovery assessment. **Probability:** High **Feature:** LAG **Function:** Port Flap Dampening & Trunk Threshold

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
103322	Medium	**Summary:** The output from the show ntp association command displays incorrect delay value. **Probability:** High **Feature:** Management **Function:** NTP
103434	Medium	**Summary:** MPLS packets are incorrectly forwarded by transit node when FRR detour is invoked. **Probability:** High **Feature:** MPLS **Function:** FRR
103438	Medium	**Summary:** A Syslog entry is not generated for ACL denied packets if ip access-group enable-deny-logging is configured on a VE interface. **Probability:** Medium **Feature:** IP Services **Function:** Access-list
103527	Medium	**Summary:** When LAG threshold is equal to the number of links in a dynamic LAG, LAG does not stabilize after disabling or enabling one of the ports. **Probability:** Medium **Feature:** LAG **Function:** Trunk Threshold
103539	High	**Summary:** Adding or modifying a cluster-id under router bgp could cause neighbors to flap. **Probability:** High **Feature:** IP Protocol **Function:** BGP
103572	Medium	**Summary:** sFlow may report incorrect sampled packet size for IP packets received on VLL end-points. **Probability:** Low **Feature:** sFlow **Function:** sFlow, VLL
103636	Medium	**Summary:** Enabling route-only on the VLL endpoints may cause the Layer 2 tunneled control packets to be dropped. **Probability:** Medium **Feature:** MPLS **Function:** VLL **Workaround:** Configure the VLL endpoints as no route-only.
103863	Medium	**Summary:** 802.1ag linktrace Reply Relay Action message format is incorrect. **Probability:** Medium **Feature:** OAM **Function:** 802.1ag
104040	High	**Summary:** A router incorrectly installs a route for IPv6 link local address if it is received in ISIS LSPs. **Probability:** High **Feature:** IP Protocol **Function:** IS-IS

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
104094	Medium	**Summary:** Traceroute should not perform reverse DNS lookup for IPv4 address when the numeric option is specified. **Probability:** Medium **Feature:** Management **Function:** Traceroute
104102	Medium	**Summary:** A router continues to send LAC-PDUs in slow timer mode after the far-end router reloads. **Probability:** Medium **Feature:** LAG **Function:** LACP
104222	High	**Summary:** A Management Module spends excessive CPU cycles in SSH when SSH key stored in chassis happens to be corrupted. **Probability:** Low **Feature:** Management **Function:** SSH
104317	High	**Summary:** Some ISIS sessions may flap under high volume of route updates. **Probability:** Medium **Feature:** IP Protocol **Function:** IS-IS
104389	Medium	**Summary:** TCP Initial Sequence Number generation does not fully conform to RFC 793. Probability : High **Feature:** IP Stack **Function:** TCP
104426	High	**Summary:** If two peer nodes in a ring topology are running 3.9.00 and 4.0.01 code respectively, interoperability issue would affect MPLS FRR detour. **Probability:** High **Feature:** MPLS **Function:** FRR
104427	Medium	**Summary:** Multicast packets may get CPU forwarded if they arrive on secondary ports of trunk on a PIM-SM RP. **Probability:** Medium **Feature:** IP Multicast **Function:** Multicast & LAG
104538	High	**Summary:** Local proxy arp does not work after line module reload. **Probability:** High **Feature:** ARP **Function:** Local-proxy-arp
104623	Medium	**Summary:** If we disable and enable LSP, BFD session for that LSP may not be added. **Probability:** Medium **Feature:** MPLS **Function:** LSP BFD
104667	Medium	**Summary:** Latency through a GE interface significantly increases upon applying 10Mbps shaper. **Probability:** High **Feature:** QoS **Function:** QoS Shaper

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
104789	Medium	**Summary:** LSP may unnecessarily flap briefly, if a user configuration removes manual selection of a secondary path, even though the primary path is not available. **Probability:** High **Feature:** MPLS **Function:** RSVP LSP
104833	High	**Summary:** A Management Module may reload while processing IGMP packet with non-zero padding received on a port that is not multicast enabled. **Probability:** Medium **Feature:** IP Forwarding **Function:** IP Forwarding
104833	High	**Summary:** A Management Module may reload while processing IGMP packet with non-zero padding that is received on port that is not multicast enabled. **Probability:** Medium **Feature:** IP Forwarding **Function:** IP Forwarding
104858	High	**Summary:** BGP peering may flap if at least one AS segment contains only private AS numbers, and the peering has remove-private-as configured, and ASN4 capability is enabled. **Probability:** Medium **Feature:** IP Protocol **Function:** BGP
104887	Medium	**Summary:** Adding the detail parameter to the end of the show ip route 0.0.0.0/0 command has no effect. **Probability:** Low **Feature:** IP Route **Function:** CLI
105076	High	**Summary:** A router may reset unexpectedly in VPLS PIM snooping operation, in an environment with a large number of multicast sessions and VPLS instances flapping. **Probability:** Medium **Feature:** Multicast Snooping **Function:** VPLS & Multicast Snooping
105098	High	**Summary:** A Management Module may reload if a router configured with radius authentication is accessed through telnet from an IPv6 Client. **Probability:** High Feature : Management **Function:** Radius
105098	High	**Summary:** A Management Module may reload if a router configured with radius authentication is accessed through telnet from an IPv6 Client. **Probability:** High **Feature:** Management **Function:** Radius
105135	Medium	**Summary:** In PIM-SM snooping, if a PIM join packet contains Joined Sources that is a higher number than the actual number of specified sources, random source IPs is selected. **Probability:** High **Feature:** IP Multicast **Function:** PIM-Sparse

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
105192	Low	**Summary:** The hw-aging disable command does not take effect after reload. **Probability:** High **Feature:** System **Function:** CLI
105196	Low	**Summary:** Partial hostnames containing a "." are presumed to be FQDNs, and no attempt is made to append the configured domain names. **Probability:** High **Feature:** Management **Function:** DNS
105238	Low	**Summary:** A Syslog message in response to power-off snm-link does not give the correct SNM number. **Probability:** High **Feature:** System **Function:** CLI
105275	High	**Summary:** BPDU or UDLD cannot be sent out when egress port is over-subscribed with tagged priority 4, 5, 6 or 7. **Probability:** Medium **Feature:** QoS **Function:** QoS
105492	Medium	**Summary:** An mroute is not getting updated when there is a more specific route available. **Probability:** Medium **Feature:** Multicast **Function:** MBGP
105530	Low	**Summary:** The console timeout does not work when a user is in User Exec mode. **Probability:** Medium **Feature:** Management **Function:** AAA
105672	Low	**Summary:** Incorrect CLI help string for ISIS default metric. **Probability:** Low **Feature:** IS-IS **Function:** CLI
105712	High	**Summary:** RPF lookup on the line card does not properly check on multicast route table. **Probability:** Medium **Feature:** Multicast **Function:** MBGP
105835	High	**Summary:** Address PIM third party interoperability when a router is the RP on a stick. **Probability:** Medium **Feature:** Multicast **Function:** PIM-Sparse
105943	Medium	**Summary:** A router should not accept Telnet or SSH access to subnet broadcast address. **Probability:** Medium **Feature:** Management **Function:** Telnet or SSH

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
106071	High	**Summary:** PRAM index gets corrupted when a GRE tunnel flaps, and its GRE tunnel's network is learned through other routing protocol. **Probability:** High **Feature:** GRE **Function:** IP-Tunnel
106080	High	**Summary:** A router may reload unexpectedly with LDP debug turned on for multiple options, and the router has sizable routes. **Probability:** Medium **Feature:** MPLS **Function:** Debug
106097	High	**Summary:** A Management CPU experiences memory leak upon SNMP Get/GetNext of snSwIfInfoGigType for any port on slot 9 or higher. **Probability:** Medium **Feature:** Management **Function:** SNMP
106120	Low	**Summary:** Syslog packets sent to the syslog server does not contain time stamp. **Probability:** Medium **Feature:** Management **Function:** Syslog
106132	Low	**Summary:** The Error: œAccess-list server address 0.0.1.0 resolved when configuring ACL with a Name instead of an IP address. **Probability:** Medium **Feature:** Access-list **Function:** DNS **Workaround:** Use access-list with ip address rather than hostnames.
106155	Low	**Summary:** Extended access-list with ipv6 protocol parameter option router-alert does not work. **Probability:** Medium **Feature:** Access-list **Function:** IP Options
106362	High	**Summary:** After LSP fails over, traffic load balancing among tunnels may not be correct. **Probability:** Medium **Feature:** MPLS **Function:** LSP Load Sharing
106558	High	**Summary:** Occasionally a directly connected VRF route is installed with an OUT label. **Probability:** Medium **Feature:** MPLS **Function:** L3VPN
106718	Low	**Summary:** If a LAG is configured with a higher port ID as its primary port, configuring sa-learning-disable feature leads to an unexpected error message. **Probability:** High **Feature:** LAG **Function:** LAG

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
106721	High	**Summary:** ISIS Redistribution scaling, Error: ISIS: Memory Limit Exceeded scrolling in log during ISIS interface flap that lasted 20 minutes. **Probability:** Medium **Feature:** IP Protocol **Function:** IS-IS
106869	Low	**Summary:** LACP log messages may display truncated information in mux state transition. **Probability:** High **Feature:** LAG **Function:** LACP
107075	Low	**Summary:** IPv6 traceroute may fail to complete when DNS server is not configured. **Probability:** High **Feature:** Management **Function:** IPv6 Traceroute **Workaround:** Configure a DNS server.
107088	Low	**Summary:** Routers configured with CDP would not transport VTP packets. **Probability:** High **Feature:** Management **Function:** CDP
107200	High	**Summary:** When the number of receivers on a multicast snoop forwarding entry exceeds 14, snooping shall be unable to correctly forward traffic for such streams. **Probability:** Medium **Feature:** Multicast **Function:** Multicast Snooping
107234	High	**Summary:** A Management Module CPU may reload unexpectedly in SNMS task when system is running low on memory and the task fails to allocate memory. **Probability:** Low **Feature:** Management **Function:** Management
107275	Low	**Summary:** The SNMP does not properly report the temperature value of the standby management module. **Probability:** High **Feature:** Management **Function:** SNMP
107393	Low	**Summary:** The output from the show ipv6 neighbor command may truncate a neighbor address if it is too long. **Probability:** Medium **Feature:** IPv6 **Function:** CLI
107501	Medium	**Summary:** Downloading of a configuration file which includes commands starting with **no** to running-config may not work if this operation is done through SNMP. **Probability:** Low **Feature:** Management **Function:** SNMP **Workaround:** Use the CLI option to download configuration files that include commands starting with **no**.

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
107606	Low	**Summary:** The output from the show chassis command may in some cases be misleading for modules that are powered off. **Probability:** Medium **Feature:** System **Function:** System
107639	Low	**Summary:** The output from the show ipv6 bgp longer-prefixes command displays incorrect routes. **Probability:** High **Feature:** BGP **Function:** CLI
107733	Low	**Summary:** If the console timeout is increased through telnet, the timeout applied to the serial connection is still between the new and the old values. Probability : Medium **Feature:** Management **Function:** Console timeout
107857	Low	**Summary:** The vlan-cpu-protection and multicast-flooding is allowed to be configured on VLAN with multicast snooping. **Probability:** High **Feature:** Multicast Snooping **Function:** CLI
108021	Medium	**Summary:** ECMP for IPv6 static routes do not properly update upon disconnection to one of the next hops. **Probability:** Medium **Feature:** IPv6 **Function:** ECMP
108063	Low	**Summary:** BGP4-MIB variables bgpPeerFsmEstablishedTime and bgpPeerInUpdateElapsedTime always returns zero value. **Probability:** High **Feature:** SNMP **Function:** MIBs
108142	Medium	**Summary:** When a VRF name is more than 14 characters, the vrf name is not correctly programmed on the line module level. **Probability:** Medium **Feature:** VRF **Function:** VRF
108283	Medium	**Summary:** A new multicast packet flow with TTL=1 would still be CPU forwarded between two VLANs, instead of being discarded. **Probability:** High **Feature:** IP Multicast **Function:** Multicast
108301	Low	**Summary:** A no vpls-peer with incorrect optional configuration would cause the vpls-peer to be deleted, even though the command was rejected. **Probability:** High **Feature:** VPLS **Function:** CLI

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
108310	Medium	**Summary:** LED for PCMCIA on 32-slot management module is not showing the correct information. **Probability:** High **Feature:** Management **Function:** PCMCIA
108340	High	**Summary:** When the (S, G) lookup fails when processing the (S, G, RPT) join, a subsequent lookup of the (*, G) may cause the router to reload unexpectedly. **Probability:** Low **Feature:** IP Multicast **Function:** PIM-Sparse
108677	High	**Summary:** The router may reload unexpectedly when the show sntp status command is executed. **Probability:** High **Feature:** Management **Function:** SNTP
109218	Low	**Summary:** Syslog and trap are not generated when a power supply is inserted or removed. **Probability:** Medium **Feature:** Management **Function:** Syslog
109301	Medium	**Summary:** A Management Module CPU may reload unexpectedly in SSH task while executing commands from the Management Module rconsole session, which is started from SSH. **Probability:** Low **Feature:** Management **Function:** SSH
109369	High	**Summary:** A router may reload unexpectedly upon executing the no module command for a slot that does not contain any module. **Probability:** Medium **Feature:** System **Function:** System
109392	High	**Summary:** On a 16-slot chassis, if the fan speed is configured manually, upon a Management module switch-over, the fan speed would be incorrectly set to low. **Probability:** High **Feature:** Management **Function:** Fans
109436	Medium	**Summary:** When a POS interface is set to OC-12, its ifhighspeed value is incorrectly returned as 0. **Probability:** High **Feature:** SNMP **Function:** MIBs
109445	Medium	**Summary:** Protocol broadcast packets such as DHCP are not subject to ACL rate-limiting. **Probability:** High **Feature:** Rate-Limit **Function:** ACL based Rate-Limit

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
109501	High	**Summary:** After repeatedly flapping the port intended for MPLS LSP primary path in FRR configuration, some LSPs may stay with their secondary path even after the port is restored. **Probability:** Medium **Feature:** MPLS **Function:** FRR
109551	Medium	**Summary:** In some cases OSPF database summary packet size may not be calculated correctly leading to issues when MD5 authentication is configured. **Probability:** Medium **Feature:** IP Protocol **Function:** OSPF
109729	Medium	**Summary:** IPv4 data packets may be assigned to the highest priority after fragmentation. **Probability:** Medium **Feature:** IPv4 forwarding **Function:** QoS
109915	Low	**Summary:** Some log entries are missing in the output of the show log ascending command. **Probability:** Medium **Feature:** Management **Function:** syslog
110203	High	**Summary:** User may experience packet loss in all the VLANs that belong to an MSTP instance after the lowest numbered member VLAN of that MSTP instance is deleted **Probability:** High **Feature:** Spanning Tree **Function:** MSTP
110222	Medium	**Summary:** The command **show ip msdp debug** may cause corruption of buffers leading to MSDP peers flap. **Probability:** Medium **Feature:** IP Multicast **Function:** MSDP **Workaround:** Avoid using the command **show ip msdp debug**
110272	Medium	**Summary:** User may see some error messages scrolling on LP console after ACL rebind, causing busy CPU. **Probability:** High **Feature:** IP Access-list **Function:** IP Access-list
110313	Medium	**Summary:** IPv4 packets that require fragmentation may be dropped by the router if route-map with deny filter is matched. **Probability:** Medium **Feature:** Policy-Based Routing **Function:** IPv4 Fragmentation
110399	Medium	**Summary:** SA-out filters may not work for SA messages that contained IP data traffic. **Probability:** Medium **Feature:** IP Multicast **Function:** MSDP **Workaround:** Configure Cisco/Juniper to not encapsulate the IP data traffic when generating MSDP SA advertisements.

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R04.1.00
105384 or 106487	High	**Summary:** A router does not Layer 2 forward any IP packet with hop-by-hop extension header. **Probability:** High **Feature:** IPV6 **Function:** IPv6 Options

Closed with Code Change Defects in the NetIron XMR and NetIron MLX Series R04.0.01

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
70870	High	**Summary:** MP may reload unexpectedly in RSVP Fast Reroute processing. **Symptom:** **Probability:** **Feature:** RSVP **Function:** Management Module
76290	High	**Summary:** A Management Module CPU may reload unexpectedly in BGP route selection operation in some special circumstances. **Symptom:** **Probability:** **Feature:** BGP **Function:** Management Module **Workaround:** Configure “always-compare-med”under “router bgp”.
76306	High	**Summary:** A Management Module may reload unexpectedly in PIM protocol processing. **Symptom:** **Probability:** **Feature:** PIM **Function:** Management Module
87703	High	**Summary:** When a user attempts to bind an outbound ACL, an error message “CAM update violation: XPP20SP 0 0x000c4ce6” appears. **Probability:** High **Feature:** IP Services **Function:** Access Lists
88472	Low	**Summary:** There is enhanced informational output for no router <protocol> commands. **Symptom:** **Probability:** **Feature:** CLI **Function:** Management Module
95252	Medium	**Summary:** SNMP temperature polling to line cards may occasionally delay link-keepalive packets causing UDLD to flap. **Symptom:** **Probability:** **Feature:** SNMP **Function:** Management Module

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
95329	Medium	**Summary:** A router does not exclude IGMP queries with 0.0.0.0 IP source address from querier election process. **Symptom:** **Probability:** **Feature:** IGMP **Function:** Management Module
95440	Medium	**Summary:** After changing the tunnel source of an IPv6 6to4 manual tunnel without first removing the source configuration, the tunnel stops receiving packets. **Symptom:** Loss of connectivity over IPv6 6to4 tunnel. **Workaround:** Disable the tunnel before changing tunnel source interface. **Probability:** Medium **Feature:** 6to4 Tunnel **Function:** IPv6 Manual Configured Tunnels **Reported in Release:** 04.0.00
95590	Medium	**Summary:** During a transition from 4000 to 8000 mcast streams, buffer errors are displayed on the console. **Symptom:** An error message is displayed in the console. **Workaround:** There is no functional impact; this is only a display issue. **Probability:** Low **Feature:** Multicast **Function:** PIM-SM **Reported in Release:** 04.0.00
95635	High	**Summary:** FRR LSPs may fail to properly clean up some resources, leading to condition where "MPLS: MAX LSP limit reached" is indicated in syslog. **Probability:** Low **Feature:** MPLS **Function:** FRR
95686	Medium	**Summary:** If a VPLS VLAN port has Layer 2 ACL binding configured, the removal of such a port to return to the default VLAN would fail. **Symptom:** **Probability:** **Feature:** ACL **Function:** Management Module
95766	Medium	**Summary:** When an IPv6 over IPv4 tunnel interface is configured for a virtual-link source interface, if the tunnel interface is removed, the virtual-link-if-address interface cannot be deleted. **Symptom:** Unable to delete virtual-link source interface configuration. **Workaround:** : First set the virtual-link source interface to some other existing interface that has a global IPv6 address configured before removing the Manual IPv6 tunnel. **Probability:** Medium **Feature:** OSPFv3 **Function:** CLI **Reported in Release:** 04.0.00
95891	Low	**Summary:** A router would erroneously allow a SFM SERDES link to come back up after it is taken down by software monitoring logic. **Symptom:** **Probability:** **Feature:** System **Function:** Management Module

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
95899	High	**Summary:** A Management Module may reload unexpectedly upon processing RSVP messages of unknown types. **Symptom:** **Probability:** **Feature:** RSVP **Function:** Management Module
95973	Medium	**Summary:** After a management switchover, some multicast streams show incorrect "in" interface information. **Symptom:** Multicast packet loss maybe seen on some streams. **Workaround:** Use the clear ip pim mcache <source> <group> command. **Probability:** Low **Feature:** Multicast **Function:** PIM-SM **Reported in Release:** 04.0.00
96045	High	**Summary:** A router may reload unexpectedly in VPLS handling upon disabling / enabling of MPLS uplink. **Symptom:** **Probability:** **Feature:** VPLS **Function:** Management Module
96054	Low	**Summary:** After a VPLS end-point port goes down, the MACs learned on such a port remains in the VPLS MAC table. **Symptom:** **Probability:** **Feature:** VPLS **Function:** Management Module
96087	High	**Summary:** Unexpected Management Module reset in RTM task during MBGP/PIM-SM configuration **Symptom:** **Probability:** **Feature:** MBGP/PIM-SM **Function:** Management Module
96129	Medium	**Summary:** If a link is restored within the “delay-link-event” time window, the Layer 2 port state is not properly changed to Forwarding. **Symptom:** **Probability:** **Feature:** CLI **Function:** Interface Module
96152	Low	**Summary:** When a VPLS end-point that is a topology group member is first brought up, its initial state should be kept as blocking. **Symptom:** **Probability:** **Feature:** VPLS **Function:** Management Module

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
96153	Low	**Summary:** If a VPLS is configured as a topology group member, IGMP packets may still be forwarded toward an end point that should be blocking. **Symptom:** **Probability:** **Feature:** IGMP **Function:** Management Module
96181	Medium	**Summary:** In some situations, the rate limited rate on NI-MLX-1Gx48T Module maybe up to 20% higher than what is expected. **Symptom:** **Probability:** **Feature:** Rate Limit **Function:** Interface Module
96248	Medium	**Summary:** A router will keep a BFD session with third party devices down, if the UDP packet checksum from the other device is all zero. **Symptom:** **Probability:** **Feature:** BFD **Function:** Management Module
96348	Medium	**Summary:** If a loopback interface originally has ip pim-sparse and/or ipv6 pim-sparse configured, and then such configurations are removed, their entries in the mroute tables are not removed accordingly. **Symptom:** **Probability:** **Feature:** PIM-SM **Function:** Management Module
96356	High	**Summary:** The output from the show media command for LX optics p/n AFCT-5715PZ-FD1 could display corrupted contents. **Probability:** Medium **Feature:** CLI **Function:** Show Media
96427	High	**Summary:** A router may reload unexpectedly upon entering the no bfd command under VPLS instance configuration level. **Symptom:** **Probability:** **Feature:** BFD **Function:** Management Module
96457	Low	**Summary:** Syslog message indicates down reason as 'unspecified' if an interface is set to be logically down due to LACP blocking. **Symptom:** **Probability:** **Feature:** Syslog **Function:** Management Module
96471	Low	**Summary:** If show mpls lsp <name> command is issued following other commands under the same LSP, the displayed status of the LSP may be incorrect. **Symptom:** **Probability:** **Feature:** MPLS **Function:** Management Module

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
96473	Low	**Summary:** The maximum allowed configurable timer for “delay-link-event” feature has been increased to 200 units. **Symptom:** **Probability:** **Feature:** CLI **Function:** Interface Module
96475	Medium	**Summary:** The ip icmp burst-normal command would also discard all IPv6 ICMP packets during lockup period, causing essential functions such as neighbor discovery to be suspended during the period. Behavior is now changed to exclude such essential packets from lockup. **Symptom:** **Probability:** **Feature:** IPv6 **Function:** Management Module
96482	Low	**Summary:** OID snBgp4NeighborSummaryRouteInstalled incorrectly shows the total number of the routes received from the peer, instead of installed routes. **Symptom:** **Probability:** **Feature:** SNMP **Function:** Management Module
96494	Low	**Summary:** Incorrect converged STP; the higher port was selected as designated port instead of lower port. **Symptom:** **Probability:** **Feature:** STP **Function:** Management Module
96666	High	**Summary:** In some cases, IGMP and PIM snooping does not work for Prune and Leave messages. **Probability:** Low **Feature:** Multicast **Function:** PIM-SM Snooping
96897	High	**Summary:** The show mpls lsp command will not show correct active path after secondary lsp is manually selected and committed. **Probability:** High **Feature:** MPLS **Function:** E-RSVP
96952	Medium	**Summary:** MPLS LSP select-path manual command may create an invalid tunnel interface. **Symptom:** **Probability:** **Feature:** MPLS **Function:** Management Module
97045	High	**Summary:** Port security may continue to enforce a deny MAC address even after the configuration is removed. **Probability:** Low **Feature:** Port Security **Function:** MAC Security

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
97082	High	**Summary:** Linecard CPU may reload unexpectedly upon hitless upgrade. **Probability:** Low **Feature:** Software Upgrade **Function:** Hitless Upgrade
97158	Medium	**Summary:** Processing of incoming L2 Trace packets could cause line cards to lose software packet buffers. **Symptom:** **Probability:** **Feature:** System **Function:** Interface Module
97195	High	**Summary:** The default route's CAM is not properly preserved upon hitless upgrade. **Probability:** High **Feature:** Hitless Upgrade **Function:** CAM mode static
97272	Medium	**Summary:** P session between two peers may fail to come up upon switch-over of peer nodes. **Symptom:** **Probability:** **Feature:** LDP **Function:** Management Module
97381	High	**Summary:** If a /32 route is flushed and updated within the minLSA interval, the LSA is re-generated with the older metric. **Probability:** Low **Feature:** L3 Routing Protocol **Function:** OSPF
97449	Medium	**Summary:** ARP pending packets in non-default VRFs may be mistakenly sent into default VRF, causing incorrect response on neighbor routers. **Symptom:** **Probability:** **Feature:** L2VPN **Function:** Management Module
97544	Medium	**Summary:** On a system already configured with rstp single, a newly configured VLAN may not have the correct collection of ports in its flooding domain. **Symptom:** **Probability:** **Feature:** RSTP **Function:** Management Module
97887	High	**Summary:** If a Layer 2 multicast packet is received at the line card CPU, which has an (S, G) entry that contains no receiver, the packet does not get properly flooded. **Probability:** High **Feature:** Multicast **Function:** L2 Multicast

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
97900	High	**Summary:** Linecard CPU reloads unexpectedly if a router is started with cam-profile set to ipv4, and system-max ifl-cam set to 81920. **Symptom:** Linecard CPU reloads unexpectedly **Probability:** High **Feature:** System **Function:** System **Reported in Release:** XMR R04.0.01 **Workaround:** If the desired CAM-profile is IPv4, configure system-max ifl-cam to 65536 or below.
98180	High	**Summary:** Clearing a targeted LDP session with non-default label space may result in inconsistency between VC labels received and advertised. **Probability:** Medium **Feature:** MPLS **Function:** LDP
98191	High	**Summary:** VRRP-E IP CAM is not deleted when the interface configuration is deleted via no interface command. **Probability:** High **Feature:** IP Protocols **Function:** VRRP-E
98464	High	**Summary:** Linecard CPU may reload unexpectedly upon adding/removing or enabling/disabling LAG port members, on LAG with rate-limiting configured. **Probability:** Low **Feature:** IP Services **Function:** Rate Limiting
98597	High	**Summary:** Cannot enable sFlow or configure sFlow global commands via INM. **Probability:** High **Feature:** Network Management **Function:** sFlow
98830	Medium	**Summary:** The qos-tos trust and qos-tos mark commands should not be allowed on VPLS end-points. **Probability:** High **Feature:** MPLS **Function:** VPLS
98960	High	**Summary:** BGP route updates with AS path greater than 251 are not installed in BGP route table. **Probability:** High **Feature:** IP Protocols **Function:** BGP
99353	High	**Summary:** The setting "ip dns domain-name" cannot remember any portion of a domain name beyond the first four characters. **Feature:** DNS **Function:** DNS CLI
99509	High	**Summary:** A Management Module CPU may reload unexpectedly upon process HTTP request that contains unstructured data more than 300 bytes. **Probability:** Medium **Feature:** Network Management **Function:** Web Management

Defect ID	Technical Severity	Closed Defects in NetIron XMR and NetIron MLX Series R4.0.01
99520	High	**Summary:** The show web-connection command does not display web user. **Probability:** High **Feature:** Network Management **Function:** Web Management
99531	High	**Summary:** A Management Module CPU may reload unexpectedly in OSPF in flushing of summary route in Appendix-E processing. **Probability:** Low **Feature:** IP Protocols **Function:** OSPF
99756	High	**Summary:** Support extensions to RFC 4893 for handling confederation path segment and other attribute errors in the new AS4_PATH and AS4_AGGREGATOR attribute. **Probability:** High **Feature:** IP Protocols **Function:** BGP
99889	High	**Summary:** A Management Module CPU may reload unexpectedly, if the show ip multicast vlan <num> command is executed immediately after disabling a port in the VLAN. **Probability:** Medium **Feature:** Multicast **Function:** IGMP Snooping
100385	High	**Summary:** A Management Module will reload unexpectedly if an RSVP LSP configured with "select-path manual" is disabled and enabled. **Probability:** Medium **Feature:** MPLS **Function:** E-RSVP
100463	High	**Summary:** Linecard CPU may reload unexpectedly if it receives a packet that needs to be copied to another packet buffer, and fails to be allocated such buffer. **Probability:** Medium **Feature:** System **Function:** CPU Buffer Management
101092	Medium	**Summary:** When system up time is at 1242 days or more, the system console may stop responding. **Probability:** Medium **Feature:** System **Function:** Interface counters

Older Closed with Code Change Defects in the NetIron XMR and NetIron MLX Series

For information regarding closed with code change defects affecting the NetIron XMR and NetIron MLX series from software releases prior to R04.0.01, please refer to earlier versions of the release notes.

Open Defects in the NetIron XMR and NetIron MLX Series R04.1.00

This section lists defects with Critical, High, and Medium Technical Severity open in Multi-Service IronWare R04.1.00 for the NetIron XMR and NetIron MLX Series Routers. While these defects are still formally “open,” they are unlikely to impede Brocade customers in their deployment of Multi-Service IronWare R04.1.00 for NetIron XMR and NetIron MLX Series Routers and have been deferred to a later release.

None of these defects have the requisite combination of probability and severity to cause significant concern to Brocade customers.

Note that when a workaround to an issue is available, it is provided; otherwise, no recommended workaround is available at this time.

Defect ID	Technical Severity	Open Defects Defects in NetIron XMR and NetIron MLX Series R04.1.00
102948	Major	**Summary: fast leave** does not work for IGMPv3 in exclude mode - works for IGMPv2, and for IGMPv3 in include mode. **Workaround:** If IGMPv3 is being used and it is in exclude mode, there is no workaround for **fast leave**; it would incur latency. Users are advised to use IGMPv2 when possible. **Probability:** High **Feature:** Multicast **Function:** IGMPv3 **Reported in Release:** XMR R04.1.00
106439	Major	**Summary:** When receivers transition from exclude to include filter mode, multicast traffic will be forwarded by interface linecard CPU. **Workaround:** Clear the corresponding (S,G) entry once it is in this state. **Probability:** High **Feature:** Multicast **Function:** IPv6 PIM-SM **Reported in Release:** NetIron XMR R04.1.00
106735	Major	**Summary:** IGMP packets entering the Provider Edge router through the VPLS tunnel will not be punted to CPU for multicast process to snoop the packet if the IGMP packet is originated by a device that is also generating a multicast stream to the same group. **Workaround:** Multicast source and multicast IGMP receiver shouldn't be configured to have the same host IP address. **Probability:** High **Feature:** Multicast **Function:** IGMP VPLS Snooping **Reported in Release:** NetIron XMR R04.1.00
107786	Major	**Summary:** When a new VPLS endpoint is created, with traffic already being forwarded to a set of existing VPLS endpoints, snooping fails to add this endpoint to its flood fid. **Workaround:** Either **clear ip multicast** or **disable/enable** of the new VPLS endpoint fixes this issue. **Probability:** High **Feature:** Multicast **Function:** IGMP VPLS Snooping **Reported in Release:** NetIron XMR R04.1.00
108445	Major	**Summary:** Enabling IGMP proxy results in VPLS peer acting as proxy for group messages received from another VPLS peer. **Workaround:** None. **Probability:** Medium **Feature:** Multicast **Function:** IGMP VPLS Snooping **Reported in Release:** NetIron XMR R04.1.00

Defect ID	Technical Severity	Open Defects Defects in NetIron XMR and NetIron MLX Series R04.1.00
109142	Medium	**Summary:** Inter-VRF IPv4 and IPv6 static routes should not get resolved via a GRE tunnel. **Workaround:** The IPv6 address set in the nexthop of a IPv6 inter-VRF static route should not be configured such that it can be resolved over a GRE tunnel or an IPv6 manual tunnel. **Probability:** Medium **Feature:** VRF **Function:** Static Routes **Reported in Release:** NetIron XMR R04.1.00
109391	Major	**Summary:** IPv6 multicast data packets of size 1452 (or 48 bytes less than the IPv6 MTU) will not be processed correctly at the RP. Consequently, the RP will fail to create (S,G) state and hardware forwarding will never be set up. **Workaround:** Use multicast data packets of size <= 1452 (or 48 bytes less than the IPv6 MTU). **Probability:** High **Feature:** Forwarding **Function:** IPv6 Forwarding **Reported in Release:** NetIron XMR R04.1.00
110508	Medium	**Summary:** When a static route/mroute points to a non-existent interface, no error is thrown although the generated configuration is invalid. **Workaround:** None **Probability:** Medium **Feature:** CLI **Function: ip mroute** **Reported in Release:** NetIron XMR R04.1.00
110581	Major	**Summary**: Upon deletion of a vrf or an interface from a VRF, any static ipv6 neighbor configured for that interface may appear under default vrf configuration in the running-configuration. **Workaround**: Delete the static ipv6 neighbor configuration before deleting the VRF or removing the interface from the VRF **Probability**: High **Feature**: VRF **Function**: CLI **Reported in Release**: XMR R04.1

Defects Affecting the NetIron CER and NetIron CES Series

Closed with Code Change Defects in the NetIron CES and NetIron CER Series R04.1.00

Defect ID	Technical Severity	Closed with Code Change Defects in the NetIron CES and NetIron CER Series R04.1.00
88540	High	**Summary:** Port in (S, G) entry created for IGMPv2 host is not deleted if host leaves a group on a coexisting IGMPv2 and v3 segment. **Symptom:** Multicast traffic may continue to flow for a limited time even though a user has left the group. **Probability:** Medium **Feature:** IGMP Snooping **Function:** IGMP **Reported in Release:** NetIron CES R03.8.00

Defect ID	Technical Severity	Closed with Code Change Defects in the NetIron CES and NetIron CER Series R04.1.00
88564	High	**Summary:** Port is not deleted from (S, G) entry if IGMPv3 host joins multicast group in exclude group and then leaves. **Symptom:** Multicast traffic may continue to flow for a limited time even though a user has left the group. **Probability:** Medium **Feature:** IGMP Snooping **Function:** IGMP **Reported in Release:** NetIron CES R03.8.00
89181	Medium	**Summary:** PIM snooping does not delete interface from (S, G) outgoing interface (oif) list after receiving (S, G) prune in case of IGMPv3 source exclude. **Symptom:** Multicast traffic may continue to flow even though a user has left the group. **Probability:** Medium **Feature:** PIM Snooping **Function:** PIM Snooping **Reported in Release:** NetIron CES R03.8.00
90488	High	**Summary:** Static client is programmed in (*,G) internal table but not in the (S, G) table after receiving multicast traffic. This issue does not occur when using dynamic clients. **Symptom:** Traffic flow does not occur from the host to the receiver. **Workaround:** Use dynamic clients when possible. **Probability:** Medium **Feature:** IGMP Snooping **Function:** IGMP **Reported in Release:** NetIron CES R03.8.00
93361	High	**Summary:** Dynamic LAG ports will be in blocked state after moving the default VLAN ID to VLAN 4089. **Probability:** High **Feature:** Dynamic LAG **Function:** LAG **Reported in Release:** NetIron CES R03.8.00
97771	Medium	**Summary:** The **show cpu average** command only reports the last 1 second average. **Probability:** High **Feature:** System **Function:** System **Reported in Release:** NetIron CES R03.8.00
100649 107580	High	**Summary:** "Power Supply 1 is bad - AC Power Supply 1 is OK" is seen on console when there is no loss of power. **Probability:** Medium **Feature:** System **Function:** System **Reported in Release:** NetIron CES R03.8.00c
101698	High	**Summary:** System resets if the command **show packet-buffer** is entered at the LP command prompt. This command is not applicable to NetIron CES. **Probability:** High **Feature:** System, Command Line **Function:** System, Command Line **Reported in Release:** NetIron CES R03.8.00

Defect ID	Technical Severity	Closed with Code Change Defects in the NetIron CES and NetIron CER Series R04.1.00
103178	High	**Summary:** Port status LEDs shut off if speed-duplex is configured for 10-half or 10-full. **Probability:** Medium **Feature:** System **Function:** System **Reported in Release:** NetIron CES R03.8.00d
103451	High	**Summary:** PIM sends out a (S,G,RPT) prune separately from (*,G) join due to a premature flush caused by another group having greater than 122 sources. **Probability:** Medium **Feature:** PIM Sparse **Function:** PIM Sparse **Reported in Release:** NetIron CES R03.8.00d
103516	Medium	**Summary: show ip pim rep-table** does not show rep-index for more than 3 digits. **Probability:** Medium **Feature:** PIM Sparse **Function:** PIM Sparse **Reported in Release:** NetIron CES R03.8.00d
103662	High	**Summary:** Under rare conditions, the command **show ip arp-mac** <*tx_id*> can cause a device to reset. **Probability:** High **Feature:** IPv4 Forwarding **Function:** IPv4 Forwarding **Reported in Release:** NetIron CES R03.8.00d
103910	Medium	**Summary:** Forwarding next hop entry is marked as drop when a port is added/removed from a VLAN. **Probability:** Medium **Feature:** VLAN **Function:** VLAN **Reported in Release:** NetIron CES R03.8.00d
103948	High	**Summary:** PIM register packet payload is mistakenly set to 0 when the first hop router encapsulates the data to the RP. **Probability:** High **Feature:** PIM Sparse **Function:** PIM Sparse **Reported in Release:** NetIron CES R03.8.00
103989	High	**Summary:** Multicast packets are duplicated at the beginning of the stream if the source and receiver are on the same VLAN port. **Probability:** High **Feature:** PIM Sparse **Function:** PIM Sparse **Reported in Release:** NetIron CES R03.8.00
104017	High	**Summary:** Miscalculation of MAC indices can cause memory corruption. **Probability:** High **Feature:** System **Function:** System **Reported in Release:** NetIron CES R03.9.00

Defect ID	Technical Severity	Closed with Code Change Defects in the NetIron CES and NetIron CER Series R04.1.00
104692	High	**Summary:** 802.1ad – DHCP packet's Inner VLAN tag is removed when processed by the CPU instead of the packet being forwarded in hardware. **Probability:** High **Feature:** 802.1ad, DHCP **Function:** 802.1ad, DHCP **Reported in Release:** NetIron CES R03.8.00c
105402	Medium	**Summary:** The **show resource** command may display erroneous values for MAC "failed" field. **Probability:** Medium **Feature:** VPLS **Function:** VPLS **Reported in Release:** NetIron CES R03.9.00
105811	High	**Summary:** ARP-MAC table entries are corrupted if an index is reused upon programming entries in the table. **Probability:** High **Feature:** System **Function:** System **Reported in Release:** NetIron CES R03.8.00d

Older Closed with Code Change Defects in the NetIron CES and NetIron CER Series

For information regarding closed with code change defects affecting the NetIron CES and NetIron CER series from software releases prior to R04.0.01, please refer to earlier versions of the release notes.

Open Defects in the NetIron CES and NetIron CER Series R04.1.00

This section lists defects with Critical, High, and Medium Technical Severity open in R04.1.00 for the NetIron CES and NetIron CER Series Routers. While these defects are still formally "open," they are unlikely to impede Brocade customers in their deployment of R04.1.00 for NetIron CES and NetIron CER Series devices and have been deferred to a later release.

None of these defects have the requisite combination of probability and severity to cause significant concern to Brocade customers.

Note that when a workaround to an issue is available, it is provided; otherwise, no recommended workaround is available at this time.

Defect ID	Technical Severity	Open Defects Defects in NetIron CES and NetIron CER Series R04.1.00
89617	Medium	**Summary:** Summarized routes may leak into NSSA as individual routes. **Symptom:** There may be additional OSPF routing table entries programmed into the system. There is no user traffic impact. **Probability:** Medium **Feature:** OSPF **Function:** OSPF **Reported in Release:** NetIron CES R03.8.00

Defect ID	Technical Severity	Open Defects Defects in NetIron CES and NetIron CER Series R04.1.00
90225	Medium	**Summary:** Router port not programmed for unknown (S, G) traffic in default VLAN and causes downstream switch not to receive traffic. **Workaround:** Always connect the multicast source to the active snooping switch. **Probability:** Medium **Feature:** IGMP Snooping **Function:** IGMP **Reported in Release:** NetIron CES R03.8.00
91145	Medium	**Summary:** NetIron CES does not process a PIM Prune message received from PIM neighbor when source and remote L2 receiver are on the same VLAN. **Symptom:** Multicast traffic may continue to flow even though a user has left the group. **Probability:** Low **Feature:** PIM Dense **Function:** PIM Dense **Reported in Release:** NetIron CES R03.8.00
105208	High	**Summary:** Traffic may be forwarded when an outbound ACL with etype IPV6 is applied on a VLL endpoint to deny traffic. **Probability:** Medium **Feature:** Access Lists **Function:** VPLS, VLL **Reported in Release:** NetIron CES R03.9.00
109822	High	**Summary:** With global Spanning Tree Protocol enabled, when adding a non-default port in an ESI VLAN with same VLAN ID of the default VLAN, the port will remain in the blocking state even though software shows it as being in the forwarding state. **Workaround**: When configuring an ESI VLAN, do not use the same VLAN ID as the configured default VLAN ID. **Probability:** High **Feature:** STP, 802.1ad, 802.1ah **Function:** STP negotiation **Reported in Release:** NetIron CES R04.1.00