HARDWARE INSTALLATION GUIDE

ExtremeRouting MLX Series Hardware Installation Guide

105018
15 June 2018

© 2018, Extreme Networks, Inc. All Rights Reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice.

Contents

Preface 9
- Document conventions 9
  - Notes, cautions, and warnings 9
  - Text formatting conventions 9
  - Command syntax conventions 10
- Extreme resources 10
- Document feedback 10
- Contacting Extreme Technical Support 11

About This Document 13
- Supported hardware and software 13
  - Supported hardware 13
  - Supported software 18
- What's new in this document 18
- How command information is presented in this guide 19
- Notice to the reader 19

Product Overview 21
- ExtremeRouting MLX Series device overview 21
- MLX Series router applications 21
- Hardware features 21
  - ExtremeRouting MLX Series routers 22
- MLX Series router modules 28
  - Management modules 28
  - Interface modules 32
  - Auto-tuning links 72
  - Forward Error Correction mode 74
  - Switch fabric modules 75
  - High-speed switch fabric modules 77
  - CFP2 to QSFP28 conversion module 77
  - Power supplies 79
  - Rack mounting brackets 81
  - Cooling system for MLX Series routers 81
  - NIBI-16-FAN-EXH-A high-speed fan assemblies 86
  - Rack mount kit 86
- Supported software features 86

Installing an ExtremeRouting MLX Series device 87
- Pre-Installation notice for the ExtremeRouting MLX chassis bundles 87
- Installation precautions 87
  - General precautions 87
  - Power precautions 89
  - Lifting precautions 91
- Installing 2x100GbE CFP2 interface modules 91
  - Installation considerations for 2x100GbE interface module 91
  - Installing 2x100GbE CFP2 interface modules 91
- Installing BR-MLX-10Gx24-DM interface modules 92
  - Installation considerations 92

Installation procedure 93
Installing an MLXe-4 router 93
Preparing the installation site 93
Unpacking an MLXe-4 router 94
Installing an MLXe-4 router in an EIA rack 94
Installing MLXe-4 router modules 97
Installing power supplies in an MLXe-4 router 99
Connecting AC power 99
Connecting DC power 100
Final steps 102
Installing an MLX-8 router 103
Preparing the installation site 103
Unpacking an MLXe-8 router 103
Installing an MLXe-8 router in an EIA rack 103
Installing the MLXe-8 router modules 105
Installing power supplies in the MLXe-8 router 107
Connecting AC power 108
Connecting DC power 109
Final steps 111
Installing an MLXe-16 router 112
Preparing the installation site 112
Unpacking an MLXe-16 router 112
Installing an MLXe-16 router in an EIA rack 113
Installing the MLXe-16 router modules 115
Installing power supplies in the MLXe-16 router 117
Connecting AC power 118
Connecting DC power 118
Final steps 120
Mounting the MLX-4, MLX-8 or MLX-16 router in a 4-post rack or EIA rack 121
EIA rack or 4-Post Rack Mount Kit contents 121
Installing MLXe-4 and MLXe-8 routers in a 4-post EIA rack 121
Installing a MLXe-16 router in a 4-post EIA rack 128
Installing an MLXe-32 router 134
Preparing the installation site 134
MLXe-32 router shipping carton contents 135
Unpacking your MLXe-32 router 135
Installing an MLXe-32 router in an EIA rack 136
Installing modules in the MLXe-32 router 152
MLXe-32 router cable management 156
Accessing modules for service 165
Installing power supplies in an MLXe-32 router 166
Connecting AC power 168
Connecting DC power 168
Removing the MLXe-32 router DC power supplies 170
Final steps 171
Attaching a management station 171
Attaching a PC or terminal to the console port or Ethernet port 171
Activating the power source 172
Verifying proper operation 172
Observing the LEDs 172

Displaying the module status.... 178
Forced card deletion.... 180

Using Extreme Structured Cabling Components.... 183
Cable cinch overview.... 183
mRJ21 procedures.... 184
Cable cinch with two mRJ21 cables.... 184
Cable cinch with three mRJ21 cables.... 184
Cable cinch with four mRJ21 cables.... 185
Cable cinch with five mRJ21 cables.... 185
Cable cinch with six mRJ21 cables.... 186
Cable cinch with seven mRJ21 cables.... 186
Cable cinch with eight mRJ21 cables.... 187
RJ-45 procedures.... 187
Cable cinch with one group of RJ-45 cables.... 188
Cable cinch with two groups of RJ-45 cables.... 188
Cable cinch with three groups of RJ-45 cables.... 189
Cable cinch with four groups of RJ-45 cables.... 189
Cable cinch with five groups of RJ-45 cables.... 190
Cable cinch with six groups of RJ-45 cables.... 190
Cable cinch with seven groups of RJ-45 cables.... 191
Cable cinch with eight groups of RJ-45 cables.... 191

Connecting a Router to a Network Device.... 193
Assigning permanent passwords.... 193
Configuring IP addresses.... 194
Support of subnet masks.... 194
Assigning an IP address to a management interface.... 195
Assigning IP addresses to an interface, virtual interface,or loopback interface.... 195
Enabling and disabling the interfaces.... 196
Understanding management port functions.... 196
Connecting the router to a network device.... 197
Installing a fiber-optic transceiver.... 197
Cabling a fiber-optic transceiver.... 198
Tunable 10 GbE DWDM SFP+.... 198
Cleaning fiber-optic ports and connectors.... 198
Troubleshooting network connections.... 198
Testing network connectivity.... 200
Pinging an IP address.... 200
Tracing a route.... 200

Managing Routers and Modules.... 201
Managing the device.... 201
Disabling and re-enabling power to interface modules.... 201
Monitoring I2C failures on management modules.... 202
Displaying device status and temperature readings.... 204
Displaying the Syslog configuration and static and dynamic buffers.... 206
Router Headless State by MP Presence from LP.... 207
Rolling Reboot.... 208
Line Module Configuration Deletion in Interactive Boot Mode.... 209
Managing switch fabric modules.... 209
Forcing HSF modules to operate in normal mode.... 210

Blocking discovery of G1 switch fabric modules....210
Managing the cooling system....210
Configuring the cooling system....210
Manually setting the fan speed....216
Monitoring the cooling system....217
Temperature log reduction....218
Managing interface modules....218
Configuring interface module boot parameters....219
Changing priority of slots for interface modules....224
Disabling and re-enabling power to interface modules....224
Monitoring Link Status....225
Enabling monitoring link status....225
Disabling monitoring link status....225
Displaying fabric link status....225
Syslog messages....226
Traffic Manager XPP link monitoring....226
Enabling TM-XPP link monitoring....227
Using alarms to collect and monitor device status....228
Configuring Alarm History Buffer Size....228
Configuring alarm logging....229
Displaying alarms....229
Clearing the alarm history log....232
Disabling SNMP trap generation and logging....232
Displaying MR2 management module memory usage....232
Enabling and disabling management module CPU usage calculations....233
Displaying CPU usage....233
Displaying management module CPU usage....234
Removing MAC address entries....235
IPv6 ND Proxy....236
IPv6 ND Proxy Configuration Tasks....237
DRBG Health Test on IPsec LP....243

Maintenance and Field Replacement....245
Maintenance and field replacement overview....245
Hardware maintenance schedule....245
Replacing a management module....246
Installing the Compact Flash Card in an MR2 management module....246
Replacing an interface module....247
Removing and replacing an interface module....247
Replacing a switch fabric module....248
Replacing a fiber-optic transceiver....248
Cabling a fiber-optic transceiver....249
Replacing a power supply....249
Determining which power supply failed....249
Setting the threshold for power supply monitoring....250
Clearing power supply failure timestamps....250
Displaying power supply monitoring timestamps....250
Enabling a power supply shutdown....252
Powering on the power supply through the CLI....252
Replacing a power supply....253
Replacing fan assemblies....255

Replacing fan assemblies in all MLXe-32 routers....255
Replacing fan assemblies in MLXe-16 routers....258
Replacing the fan tray assembly in MLXe-4 and MLXe-8 routers....259
Replacing the air filters....262
Installing upward deflectors on fan assemblies....265

Hardware Specifications....271
Hardware specifications for ExtremeRouting MLX Series routers....271
Power specifications....271
Physical dimensions....273
Operating environment....274
Storage environment....274
Safety agency approvals....274
Electromagnetic approvals....275
Port specifications for all router models....275
2x100GbE CFP2 Dynamic Port Configuration....275
Console port pin assignments....275
Management port pin assignments....276

ExtremeRouting MLX Series Chassis Bundles....277

Regulatory Statements....287
BSMI statement (Taiwan)....287
Canadian requirements....287
China CC statement....288
Europe and Australia (CISPR 22 Class A Warning)....288
FCC warning (US only)....289
Germany....289
KCC statement (Republic of Korea)....289
VCCI statement....290
Japan power cord....290
EMC, safety, and environmental regulatory compliance information....290
Regulatory compliance (EMC)....290
Regulatory compliance (safety)....291
Regulatory compliance (environmental)....291

Caution and Danger Notices....293
Cautions....293
General cautions....293
Electrical cautions....294
Cautions related to equipment weight....300
Danger Notices....301
General dangers....301
Electrical dangers....301
Dangers related to equipment weight....304
Laser dangers....305

Preface

- Document conventions 9
- Extreme resources 10
- Document feedback 10
- Contacting Extreme Technical Support 11

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Extreme resources

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

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

Document feedback

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

You can provide feedback in two ways:

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

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

Contacting Extreme Technical Support

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

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

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

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

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

About This Document

- Supported hardware and software....13
- What's new in this document....18
- How command information is presented in this guide....19
- Notice to the reader....19

Supported hardware and software

The following sections describe the supported hardware and software for this document. If procedures or parts of procedures apply to some devices but not to others, this guide identifies which devices are supported and which are not.

Although many different hardware configurations are tested and supported by Extreme, documenting all possible configurations and scenarios is beyond the scope of this document.

Supported hardware

This document describes hardware installation and troubleshooting procedures for the following ExttremeRouting MLX Series hardware platforms:

- ExtremeRouting MLXe-4 router
- ExtremeRouting MLXe-8 router
- ExtremeRouting MLXe-16 router
- ExtremeRouting MLXe-32 router

The following table describes all supported management modules for the MLX Series routers.

TABLE 1 Management modules used with MLX Series routers

Part number	Description	Supported devices	Introduced	Supported	Notes
BR-MLX-MR2-M	(MR2) Gen2 management (M). 4 GB RAM, 1 internal 2 GB CF drive, 1 external CF slot, 2 GB card (included), RS-232 serial console port and 10/100/1000 Ethernet port.	MLXe-4, MLXe-8 and MLXe-16 MLX-4, MLX-8 and MLX-16	Extreme NetIron R05.7.xx.	Yes	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-MR2-X	(MR2) Gen2 management (X). 4 GB RAM, 1 internal 2 GB CF drive, 1 external CF slot, 2 GB card (included), RS-232 serial console port and 10/100/1000 Ethernet port.	MLXe-4, MLXe-8 and MLXe-16	Extreme NetIron R05.7.xx.	Yes	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-32-MR2-M	(MR2) Gen2 management (M). 4 GB RAM, 1 internal 2 GB CF drive, 1 external CF slot, 2 GB card (included), RS-232 serial console port and 10/100/1000 Ethernet port.	MLXe-32 MLX-32	Extreme NetIron R05.7.xx.	Yes	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-32-MR2-X	(MR2) Gen2 management (X). 4 GB RAM, 1 internal 2 GB CF drive, 1 external CF slot, 2 GB card (included), RS-232 serial console port and 10/100/1000 Ethernet port.	MLXe-32	Extreme NetIron R05.7.xx.	Yes	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.

TABLE 1 Management modules used with MLX Series routers (continued)

Part number	Description	Supported devices	Introduced	Supported	Notes
NI-MLX-MR	(MR) management module, 1 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports.	MLXe-4, MLXe-8 and MLXe-16 MLX-4, MLX-8 and MLX-16	Extreme NetIron R05.2.00.	Extreme NetIron R05.7.xx.	EOL initiated.
NI-MLX-32-MR	(MR)-32 management module, 1 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports.	MLXe-32 MLX-32	Extreme NetIron R05.2.00.	Extreme NetIron R05.7.xx.	EOL initiated.
NI-XMR-MR	(MR) management module, 2 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports.	MLXe-4, MLXe-8 and MLXe-16	Extreme NetIron R05.2.00.	Extreme NetIron R05.7.xx.	EOL initiated.
NI-XMR-32-MR	(MR)-32 management module, 2 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports.	MLXe-4, MLXe-8 and MLXe-16	Extreme NetIron R05.2.00.	Extreme NetIron R05.7.xx.	EOL initiated.

The following table describes all supported interface modules for the MLX Series routers.

TABLE 2 Interface modules used with MLX Series routers

Part number	Description	Supported device(s)	Introduced	Supported	Notes
BR-MLX-100GX1-X	One (1)-port 100 GbE (X) module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode.	MLXe-4, MLXe-8 and MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Extreme NetIron R05.6.00e.	Yes	Requires CFP optics and high speed switch fabric modules. License ungradable to 2 ports on MLXe.
BR-MLX-100GX2-CFP2-M	Two (2)-port 100 GbE (M) module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.7.00.	Yes	Requires CFP2 optics and high speed switch fabric modules.
BR-MLX-100GX2-CFP2-X2	Two (2)-port 100 GbE (X2) module with IPv4/IPv6/MPLS hardware support. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.7.00.	Yes	Requires CFP2 optics and high speed switch fabric modules.
BR-MLX-100GX2-X	2-port 100-GbE (X) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.6.00e.	Yes	Requires CFP optics and high speed switch fabric modules.
BR-MLX-10GX4-IPSEC-M	Eight port (4-port 10-GbE and 4-port 1-GbE) (M) IP Security (IPSEC) module with IPv4/IPv6/VRF hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.8.00.	Yes	Requires SFP+ and SFP optics and high speed switch fabric modules.
BR-MLX-10Gx20-M	Twenty (20)-port 10-GbE/1-GbE (M) combo module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.7.00.	Yes	Requires SFP+ and SFP optics and high speed switch fabric modules.
BR-MLX-10Gx20-X2	Twenty (20)-port 10-GbE/1-GbE (X2) combo module with IPv4/IPv6/MPLS hardware support. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.7.00.	Yes	Requires SFP+ and SFP optics and high speed switch fabric modules.

TABLE 2 Interface modules used with MLX Series routers (continued)

Part number	Description	Supported device(s)	Introduced	Supported	Notes
NI-MLX-10GX2	2-port 10-GbE module with IPv4/IPv6/MPLS hardware support.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Earlier than NetIron R05.1.00.	Extreme NetIron R05.6.00.	EOL initiated. Requires XFP optics.
NI-MLX-10GX4	4-port 10-GbE module with IPv4/IPv6/MPLS hardware support.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Earlier than NetIron R05.1.00.	Extreme NetIron R05.6.00.	EOL initiated. Requires XFP optics.
BR-MLX-10GX4-X	4-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.1.00f. Extreme NetIron R05.2.00e. Extreme NetIron R05.3.00b.	Yes	Requires XFP optics.
BR-MLX-10Gx4-X-ML	4-port 10-GbE (ML) module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Extreme NetIron R05.1.00f. Extreme NetIron R05.2.00e. Extreme NetIron R05.3.00b.	Yes	Requires XFP optics. License Upgradable to "X" scalability (1M IPv4 routes in FIB).
BR-MLX-40Gx4-M	4-port 40-GbE (M) module with Layer 2, IPv4/IPv6, MPLS and OpenFlow. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.6.00.	Yes	Requires QSFP+ optics and high speed switch fabric modules.
NI-MLX-10GX8-M	MLX Series 8-port 10-GbE (M) module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Extreme NetIron R05.0.00.	Yes	Requires SFP optics and high speed switch fabric modules.
NI-MLX-10GX8-D	MLX Series 8-port 10-GbE (M) module with IPv4/IPv6 hardware support. Supports 256K IPv4 routes in FIB. Doesn't support MPLS.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Extreme NetIron R05.0.00.	Yes	EOL initiated. Requires SFP optics and high speed switch fabric modules.
BR-MLX-10GX8-X	8-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.2.00.	Yes	Requires SFP optics and high speed switch fabric modules.
NI-MLX-1GX20-SFP	20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00. EOL initiated. Support discontinued.	Requires SFP optics. Copper SFPs are supported at 1000Mbps only.
NI-XMR-1GX20-SFP	20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support.		Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00. EOL initiated. Support	Requires SFP optics. Copper SFPs are supported at 1000Mbps only.

TABLE 2 Interface modules used with MLX Series routers (continued)

Part number	Description	Supported device(s)	Introduced	Supported	Notes
				discontinued.	
NI-MLX-1GX20-GC	20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.	MLX-4, MLX-8 MLX-16 and MLX-32	Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00. EOL initiated. Support discontinued.	
NI-XMR-1Gx20-GC	20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.		Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00. EOL initiated. Support discontinued.	
BR-MLX-1GCX24-X	24-port 10/100/1000 Copper (RJ-45) Module with IPv4/ IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	MLX-4, MLX-8 MLX-16 and MLX-32	Earlier than Extreme NetIron R05.9.00.	Yes	
BR-MLX-1GCX24-X-ML	24-port 10/100/1000 Copper (RJ-45) Module with IPv4/ IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Earlier than Extreme NetIron R05.4.00.	Yes	License Upgradable to "X" scalability (1M IPv4 routes in FIB).
BR-MLX-1GFX24-X	24-port 1-GbE Fiber (SFP) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Earlier than Extreme NetIron R05.4.00.	Yes	
BR-MLX-1GFX24-X-ML	24-port 1-GbE Fiber (SFP) Module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Earlier than Extreme NetIron R05.4.00.	Yes	License Upgradable to "X" scalability (1M IPv4 routes in FIB).
BR-MLX-10GX24-DM	24-port 10-GbE Module with IPv4/IPv6/ MPLS hardware support. Bandwidth up to 200Gbps per module. Supports 256K IPv4 routes.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32	Extreme NetIron R05.4.00.	Yes	Requires SFP optics.
NI-MLX-1GX48-T-A	48-port 10/100/1000Base-T, MRJ21 module with IPv4/IPv6/MPLS hardware support.	MLXe-4, MLXe-8 MLXe-16 and MLXe-32 MLX-4, MLX-8 MLX-16 and MLX-32	Earlier than Extreme NetIron R05.4.00.	Yes	Requires high speed fans NIBI-16-FAN-EXH-A on MLX-16.

The following table describes all supported switch fabric modules for the MLX Series routers.

TABLE 3 Switch fabric modules used with MLX Series routers

Part number	Description	Supported device(s)	Introduced	Supported	Notes
NI-X-4-HSF	High speed switch fabric module	MLXe-4 MLX-4	Earlier than Extreme NetIron R05.4.00.	Yes	
NI-X-16-8-HSF	High speed switch fabric module	MLXe-8, MLXe-16 MLX-8, MLX-16	Earlier than Extreme NetIron R05.4.00.	Yes	
NI-X-32-HSF	High speed switch fabric module	MLXe-32 MLX-32	Earlier than Extreme NI R05.4.00.	Yes	
NI-X-SF1	Switch fabric module	MLXe-4 MLX-4	Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00.	EOL initiated.
NI-X-SF3	Switch fabric module	MLXe-8, MLXe-16 MLX-8, MLX-16	Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00.	EOL initiated.
NI-X-32-SF	Switch fabric module	MLXe-32 MLX-32	Extreme NetIron R05.2.00.	Extreme NetIron R05.6.00.	EOL initiated.

The following table describes all supported power supplies for the MLX Series routers.

TABLE 4 Power supplies used with MLX Series routers

Part number	Description	Supported device(s)	Introduced	Supported	Notes
XBR-ACPWR-1800	AC 1800W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16		Yes	
XBR-DCPWR-1800	DC 1800W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16		Yes	
BR-MLXE-ACPWR-1800	AC 1800W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16	Extreme NetIron R05.4.00. or earlier	Yes	
BR-MLXE-DCPWR-1800	DC 1800W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16	Extreme NetIron R05.4.00. or earlier	Yes	
NI-X-ACPWR	AC 1200W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.
NI-X-DCPWR	DC 1200W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.
NI-X-ACPWR-A	AC 1200W power supply.	MLXe-4, MLXe-8 and MLXe-16 MLX-8 and MLX-16	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.
NI-X-DCPWR-A	1200W power supply.	MLXe-4, MLXe-8 and MLXe-16	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.

TABLE 4 Power supplies used with MLX Series routers (continued)

Part number	Description	Supported device(s)	Introduced	Supported	Notes
		MLX-8 and MLX-16			
BR-MLXE-32-ACPWR-3000	AC 3000W power supply.	MLXe-32 MLX-32	Extreme NetIron R05.4.00. or earlier	Yes	
BR-MLXE-32-DCPWR-3000	DC 3000W power supply.	MLXe-32 MLX-32	Extreme NetIron R05.4.00. or earlier	Yes	
NIBI-32-ACPWR-A	AC 2400W power supply.	MLXe-32 MLX-32	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.
NIBI-32-DCPWR	DC 2400W power supply.	MLXe-32 MLX-32	Extreme NetIron R05.4.00. or earlier	EOL initiated.	Not available for purchase.

The following table describes all rack mount kits for the MLX Series routers.

TABLE 5 Rack mount kits used with MLX Series routers (OS-independent)

Part number	Description	Supported device(s)	Notes
RMK-4POST-MLXE-32	4-post rack mount kit	MLXe-32	Flush mount installation
RMK-CAB-CTO-MLXE-32	4-post rack mount kit	MLXe-32	Custom Federal Rack/ Cabinet (CTO)
RMK-CAB-MLXE-16	Kit for installation in a cabinet or a 4-post rack	MLXe-16	Includes a Cable Management Comb for cable management
RMK-CAB-MLXE-32	Rack-mount kit for installation in a cabinet	MLXe-32	Recess kit
RMK-CAB-MLXE-4	Kit for installation in a cabinet or a 4-post rack	MLXe-4	
RMK-CAB-MLXE-8	Kit for installation in a cabinet or a 4-post rack	MLXe-8	
RMK-NI-X-32	Kit for installation in a standard 2-post rack	MLXe-32 MLX-32 XMR32000	

Supported software

This document is specific to the MLX Series routers running Extreme NetIron software release 6.0.00 and later.

What's new in this document

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks., Inc., as appropriate.

How command information is presented in this guide

Starting with Extreme NetIron 5.6.00, command syntax and parameter descriptions are removed from commands that are referenced in configuration tasks. To find the full description of a specific command, including all required and optional keywords and variables, refer to the *Extreme NetIron Command Reference* for your software release.

Notice to the reader

This document contains references to Phillips screws. This trademark is the property of the Phillips Screw Company, Inc.

This reference is made for informational purposes only.

Product Overview

- ExtremeRouting MLX Series device overview....21
- MLX Series router applications....21
- Hardware features....21
- MLX Series router modules....28
- Supported software features....86

ExtremeRouting MLX Series device overview

The MLX Series routers provide high-performance routing to service providers, distributed enterprises, and research networks, offering the following benefits:

- Scalable multi-service IP/MPLS carrier Ethernet routers
- 100-Gbps Ethernet, 10-Gbps Ethernet and 1-Gbps Ethernet wire speed ports in a single router
- Wire-speed IPv4, IPv6, and MPLS forwarding performance
- Comprehensive IPv4 and IPv6 routing support based on Extreme NetIron operating system
- High-availability design with redundant management modules, switch fabric modules, power supplies and fans, supporting hitless failover, hitless software upgrades, and non-stop routing
- Advanced, scalable Metro Ethernet Layer 2 services
- Advanced Layer 2/Layer 3 VPN and multicast capabilities supporting residential triple-play and business services
- Comprehensive hardware-based security and policies
- Advanced QoS for differentiated SLAs

MLX Series router applications

MLX Series routers are commonly deployed in the following situations:

- Layer 2 metro networks
- Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) service provider networks supporting multi-VRFs and RFC 2547bis
- MPLS Layer 2 VPN service provider networks supporting both Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL)
- MPLS backbone "P" routers
- Data centers
- Enterprise backbones

Hardware features

This section describes the available hardware components of the MLX Series routers, including the slots available in the chassis for each component. For installation instructions, refer to the Installing an ExtremeRouting MLX Series device on page 87.

ExtremeRouting MLX Series routers

MLX Series routers are available in the following models:

- MLXe-4: 4 interface slots (refer to MLXe-4 router components on page 22)
- MLXe-8: 8 interface slots (refer to MLXe-8 router components on page 23)
- MLXe-16: 16 interface slots (refer to MLXe-16 router components on page 23)
- MLXe-32: 32 interface slots (refer to MLXe-32 router components on page 26)

The following content describes the components you can install in the router slots, and the numbering scheme used for those slots. For a detailed list of components that ships with each router, refer to ExtremeRouting MLX Series Chassis Bundles on page 277.

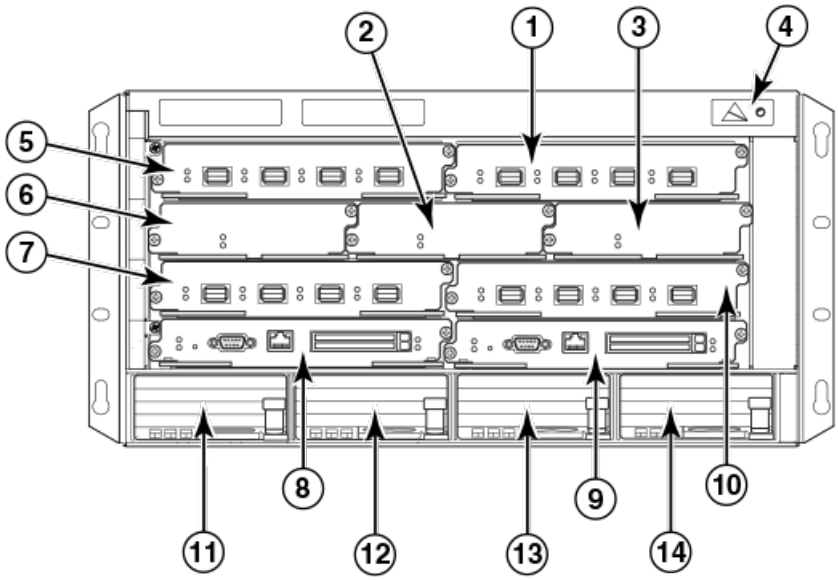
MLXe-4 router components

You can install the following components in the router slots:

- Up to two management modules (one active and one redundant).
- Up to three switch fabric modules.
- Up to four interface modules.
- Up to four power supplies (AC or DC).

For a detailed list of components that ships with each router, refer to ExtremeRouting MLX Series Chassis Bundles on page 277.

FIGURE 1 MLXe-4 router



1. Interface slot 2
2. Switch fabric slot 2
3. Switch fabric slot 3
4. ESD connector
5. Interface slot 1
6. Switch fabric slot 1
7. Interface slot 3
8. Management slot 1
9. Management slot 2
10. Interface slot 4
11. Power supply 1
12. Power supply 2
13. Power supply 3
14. Power supply 4

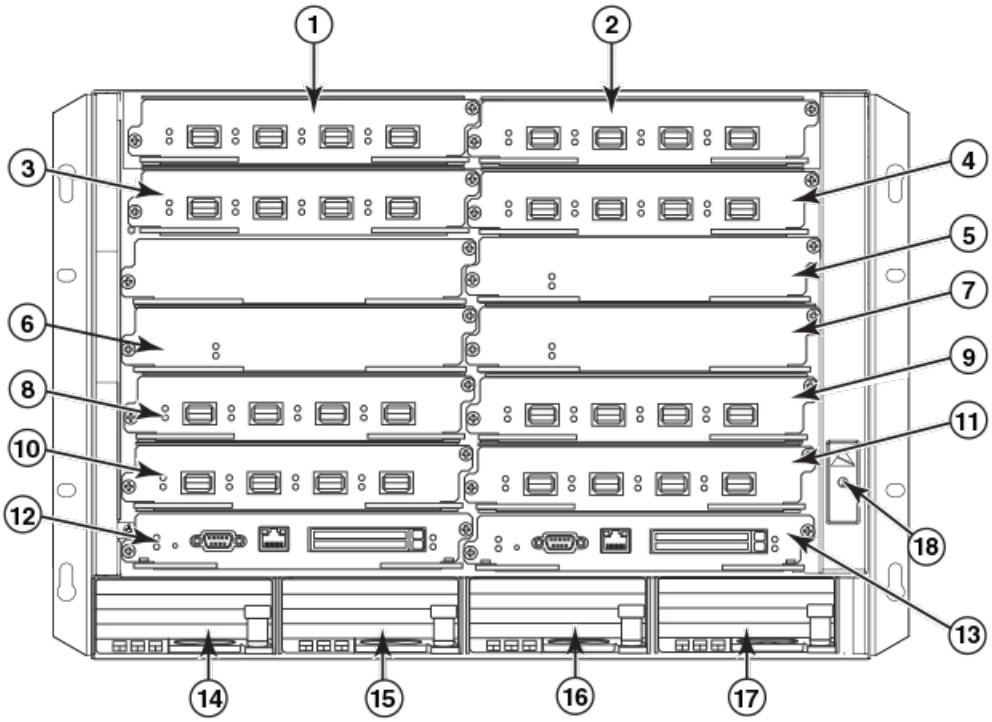
MLXe-8 router components

You can install the following components in the router slots:

- Up to two management modules (one active and one redundant).
- Up to three switch fabric modules.
- Up to eight interface modules.
- Up to four power supplies (AC or DC).

For a detailed list of components that ships with each router, refer to ExtremeRouting MLX Series Chassis Bundles on page 277.

FIGURE 2 MLXe-8 router



1. Interface slot 1
2. Interface slot 2
3. Interface slot 3
4. Interface slot 4
5. Switch fabric slot 1
6. Switch fabric slot 2
7. Switch fabric slot 3
8. Interface slot 5
9. Interface slot 6
10. Interface slot 7
11. Interface slot 8
12. Management slot 1
13. Management slot 2
14. Power supply slot 1
15. Power supply slot 2
16. Power supply slot 3
17. Power supply slot 4
18. ESD connector

MLXe-16 router components

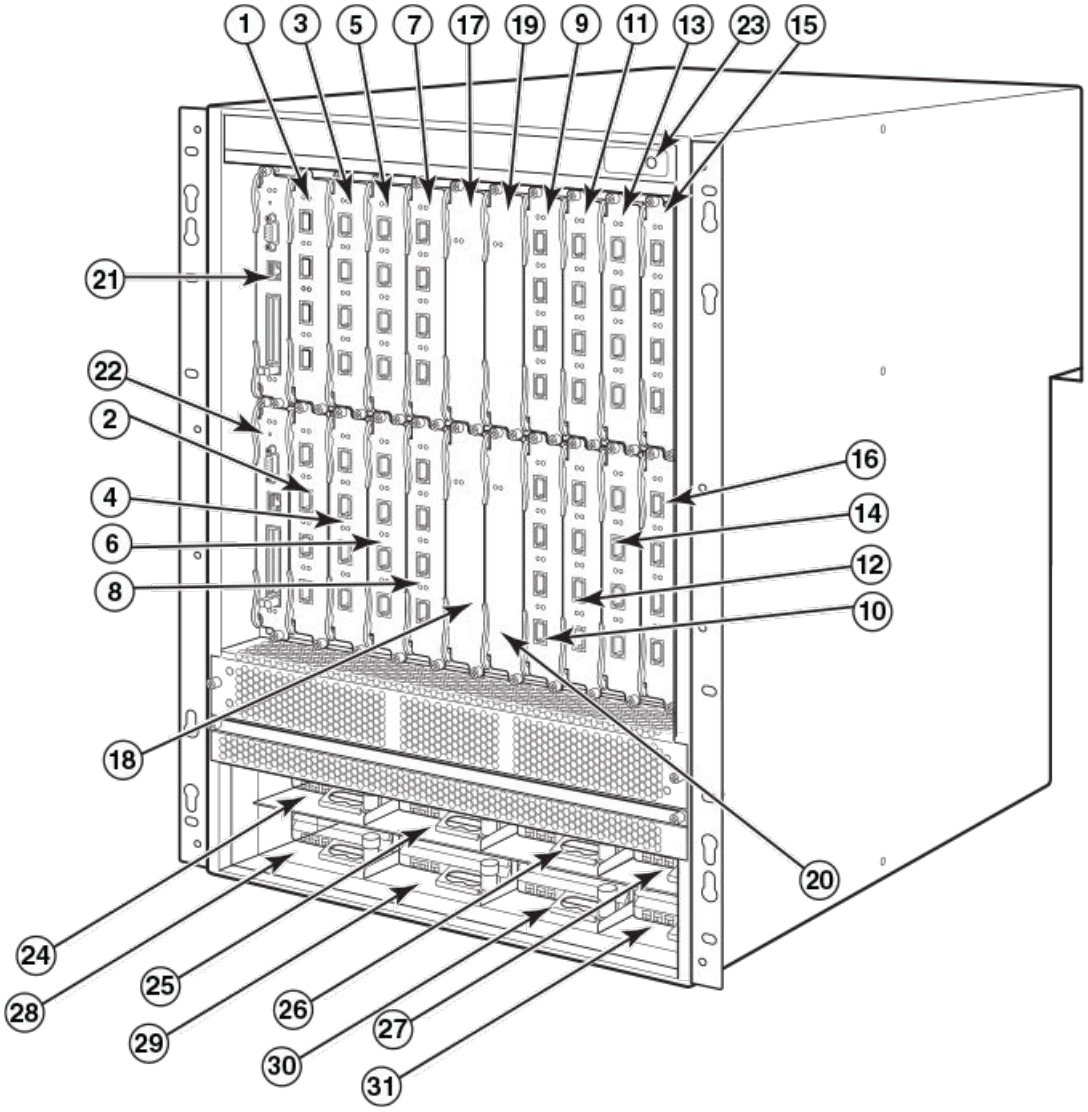
You can install the following components in the router slots:

- Up to two management modules (one active and one redundant).

- Up to four switch fabric modules.
- Up to 16 interface modules.
- Up to eight power supplies (AC or DC).

For a detailed list of components that ships with each router, refer to ExtremeRouting MLX Series Chassis Bundles on page 277.

FIGURE 3 MLXe-16 router



1. Interface slot 1
2. Interface slot 2
3. Interface slot 3
4. Interface slot 4
5. Interface slot 5
6. Interface slot 6
7. Interface slot 7
8. Interface slot 8
9. Interface slot 9
10. Interface slot 10
11. Interface slot 11
12. Interface slot 12
13. Interface slot 13
14. Interface slot 14
15. Interface slot 15
16. Interface slot 16
17. Switch fabric slot 1
18. Switch fabric slot 2
19. Switch fabric slot 3
20. Switch fabric slot 4
21. Management slot 1
22. Management slot 2
23. ESD connector
24. Power supply slot 1
25. Power supply slot 2
26. Power supply slot 3
27. Power supply slot 4
28. Power supply slot 5
29. Power supply slot 6
30. Power supply slot 7
31. Power supply slot 8

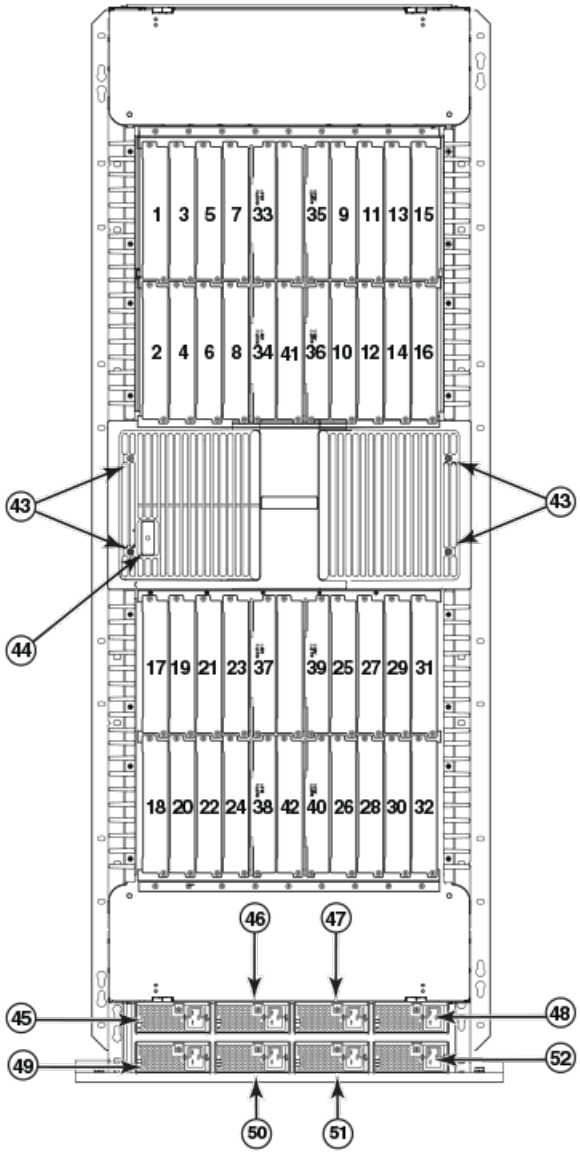
MLXe-32 router components

You can install the following components in the router slots:

- – Up to two management modules.
  – Up to eight switch fabric modules.
  – Up to 32 interface modules.
  – Up to eight power supplies (AC or DC).

For a detailed list of components that ships with each router, refer to ExtremeRouting MLX Series Chassis Bundles on page 277.

FIGURE 4 MLXe-32 router



1. Interface slot 1
2. Interface slot 2
3. Interface slot 3
4. Interface slot 4
5. Interface slot 5
6. Interface slot 6
7. Interface slot 7
8. Interface slot 8
9. Interface slot 9
10. Interface slot 10
11. Interface slot 11
12. Interface slot 12
13. Interface slot 13
14. Interface slot 14
15. Interface slot 15
16. Interface slot 16
17. Interface slot 17
18. Interface slot 18
19. Interface slot 19
20. Interface slot 20
21. Interface slot 21
22. Interface slot 22
23. Interface slot 23
24. Interface slot 24
25. Interface slot 25
26. Interface slot 26
27. Interface slot 27
28. Interface slot 28
29. Interface slot 29
30. Interface slot 30
31. Interface slot 31
32. Interface slot 32
33. Switch fabric slot 1
34. Switch fabric slot 2
35. Switch fabric slot 3
36. Switch fabric slot 4
37. Switch fabric slot 5
38. Switch fabric slot 6
39. Switch fabric slot 7
40. Switch fabric slot 8
41. Management slot 1
42. Management slot 2
43. Captive screws
44. ESD connector
45. Power supply slot 1
46. Power supply slot 2
47. Power supply slot 3
48. Power supply slot 4
49. Power supply slot 5
50. Power supply slot 6
51. Power supply slot 7
52. Power supply slot 8

MLX Series router modules

The MLX Series routers support a number of management modules, interface modules, and switch fabric modules, as shown in the following content.

Management modules

MLX Series routers support the following management modules types.

- MR management module
- MR2 management module

The following table lists the management modules available for MLX Series routers.

TABLE 6 Management modules for all MLX Series routers

Part number	Description	Notes
NI-MLX-MR	(MR) MLX Series and MLX Series management module, 1 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.	This module is no longer supported from Extreme NetIron R05.7.xx.

TABLE 6 Management modules for all MLX Series routers (continued)

Part number	Description	Notes
NI-MLX-32-MR	(MR) MLX SeriesMLXe-32 and MLX Series-32 management module, 1 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.	This module is no longer supported from Extreme NetIron R05.7.xx.
NI-XMR-MR	(MR) XMR Series management module, 2 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.	This module is no longer supported from Extreme NetIron R05.7.xx.
NI-XMR-32-MR	(MR) XMR Series 32000 management module, 2 GB SDRAM, dual auxiliary flash slots, EIA or TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.	This module is no longer supported from Extreme NetIron R05.7.xx.
BR-MLX-MR2-M	(MR2) MLXe/MLX Gen2 management (M) module for 4-, 8- and 16-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2 GB), 1 external compact flash slot with included 2 GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-MR2-X	(MR2) MLXe/XMR Gen2 management (X) module for 4-, 8- and 16-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2 GB), 1 external compact flash slot with included 2 GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-32-MR2-M	(MR2) MLXe Gen2 management (M) module for 32-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2 GB), 1 external compact flash slot with included 2 GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.
BR-MLX-32-MR2-X	(MR2) MLXe/XMR Gen2 management (X) module for 32-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2 GB), 1 external compact flash slot with included 2 GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.	You must use one of the relevant MR2 modules starting from Extreme NetIron R05.8.00.

The management module controls the hardware components, runs the networking protocols, and provides the Real Time Operating System (RTOS).

Each router requires one management module, and can accommodate a second module for redundancy. A redundant management module works in conjunction with the active management module. If the active module becomes unavailable, the redundant management module automatically takes over the system operation, minimizing system downtime. For information about the redundancy feature, refer to the *Extreme NetIron Switching Configuration Guide*.

Management modules are installed in dedicated slots marked M1 and M2. By default, the module installed in slot M1 is the active management module.

Management modules are hot-swappable, which means you can remove and replace them without powering down the system.

NOTE
MR and MR2 management modules cannot be mixed in the same chassis.

NOTE
Prior to installing or replacing the MR2 management module, you must read the Hardware Installation Notes that shipped with the hardware.

NOTE
Although management modules are designed to be hot-swappable, you must upgrade the software on all interface modules and management modules to the appropriate software release before installing them. For more information on the appropriate software release, refer to the Hardware Installation Notes that shipped with the management module.

FIGURE 5 MR management module front panel

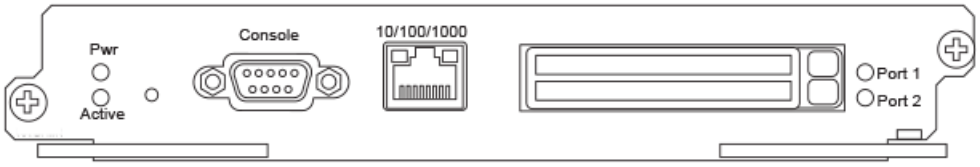
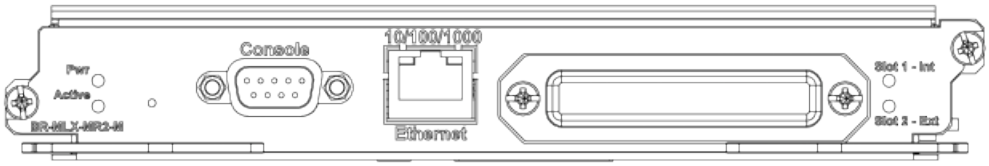


FIGURE 6 MR2 management module front panel



The front panel of the management module contains the following features:

- Two auxiliary flash slots (available on MR management modules only)
- Compact flash slot (available on MR2 management modules only)
- Console port
- A 10/100/1000 Ethernet port
- Six LEDs

Auxiliary flash slots

Auxiliary flash slots support flash PC cards where you can store boot images, startup and running configuration files, and other system files, in addition to what is stored in system flash memory. This allows you to perform system management tasks, such as copying files between flash PC cards, or copying files between a flash PC card and flash memory.

For maximum performance, it is recommended that you use Extreme auxiliary flash cards, part number FLASH-PCC, which can be ordered from Extreme Networks. Extreme auxiliary flash cards ship with the label on the bottom of the card; take caution to insert the card with the label on the bottom side.

NOTE
Some older auxiliary flash cards can be inserted the wrong way in the slot because there is no indication in the card about which is the right way. If you insert the card backwards, you will see continuous messages in the console and the card inserted/ card removed syslog. If this occurs, you must remove the card and reinsert it the correct way.

External compact flash

MR2 management modules do not contain an auxiliary flash slot. Instead, they contain a 2 GB internal compact flash card and an external compact flash drive. MR2 management modules come with a factory installed compact flash card in the external compact flash slot. The internal compact flash provides greater storage space for image retention, improving the upgrade process.

> **NOTE**
> Do not use compact flash cards over 2 GB; they will render the system unstable.The internal compact flash card cannot be accessed for removal or replacement.

The external compact flash slot allows you to insert a 2 GB compact flash card. If you need to replace or add an additional compact flash card, contact Extreme technical support.

Console port

The console port is a standard DB-9 serial connector through which you can attach a PC or terminal to configure the router using the CLI.

> **NOTE**
> The console port interfaces the control plane only. It does not interface the data plane.

10/100/1000 Ethernet port

Management modules contain a 10BaseT, 100BaseTX, or 1000BaseTX auto-sensing, auto-negotiating Ethernet port. This port has an RJ-45 unshielded twisted pair (UTP) connector.

Typical uses of this port include, but are not limited to, the following:

- Connecting a PC to configure, monitor, and manage the system through a Telnet or SSHv2 connection.
- Connecting to the 10BaseT, 100BaseTX, or 1000BaseTX port for connectivity to your existing management network. You can then access the router and configure, monitor, and manage the system from a management station.

> **NOTE**
> The existing management network into which you can connect the 10/100/1000 Ethernet port must be separate and isolated from the network over which user packets are switched and routed. For information about the functionality of the management port, refer to Understanding management port functions on page 196.

For information about connecting a PC to the 10/100/1000 Ethernet port, refer to Attaching a management station on page 171.

The out-of-band management port provides access to a separate system management network, and allows the ability to perform the following tasks:

- Access the router through SSH, Telnet, the Web management interface, or Extreme Network management software.
- Access a TFTP server to perform system upgrade tasks.
- Configure SNMP polling access.
- Send SNMP traps.
- Send Syslog packets.
- Access the system through RADIUS AAA.

Management module LEDs

The LEDs on all management module models are the same. The following table describes the LEDs on the management module.

TABLE 7 Management module LEDs

LED	Position	State	Meaning
Port 1 and Port 2	Each adjacent to the auxiliary flash slot that it represents	On or blinking	The software is currently accessing the auxiliary flash card.
		Off	The software is not currently accessing an auxiliary flash card, although there is one inserted in the slot.
Active	Lower Left	On	The module is functioning as the active management module.
		Off	The module is functioning as the redundant management module.
Pwr	Upper Left	On	The module is receiving power.
		Off	The module is not receiving power.
10/100/1000 Ethernet Port	Above and right of RJ-45 connector	On (Green)	A link is established with the remote port.
		Off	No link is established with the remote port.
10/100/1000 Ethernet Port	Above and left of RJ-45 connector	On or blinking (Yellow)	The port is transmitting and receiving packets.
		Off for an extended period	The port is not transmitting or receiving packets.

Pre-installation notice for MLX Series chassis bundles with MR2 management modules

The following conditions must be met for any chassis with a MR2 management module to operate properly.

- The MR2 module requires a minimum Extreme NetIron software version R05.2.00b to operate. Do not attempt to downgrade the MR2 module to a release lower than R05.2.00b.
- MR2-M and MR2-X modules cannot be mixed together in any MLX Series chassis
- MR and MR2 modules cannot be mixed together in any MLX Series chassis
- Do not downgrade the MBRIDGE version on the MR2 module.
  - The MR2 management module requires MBRIDGE version 36 or later for 4-, 8-, and 16-slot devices
  - The MR2 management module requires MBRIDGE32 version 35 or later for 32-slot devices
- In certain module combinations, you will need to make sure the supported software is loaded.

Interface modules

Three generations of interface modules exist for MLX Series routers.

The following table lists interface modules that are available for MLX Series routers.

TABLE 8 Interface modules for all MLX Series routers

SKU	Ports	Description	Generation
BR-MLX-100GX2-CFP2-M	2	MLXe two (2)-port 100-GbE (M) module with IPv4/IPv6/MPLS hardware support. Requires CFP2 optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules.	Gen 3
BR-MLX-100GX2-CFP2-X2	2	MLXe two (2)-port 100-GbE (X2) module with IPv4/IPv6/MPLS hardware support. Requires	Gen 3

TABLE 8 Interface modules for all MLX Series routers (continued)

SKU	Ports	Description	Generation
		CFP2 optics. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB. Requires high speed switch fabric module.	
BR-MLX-10Gx20-M	20	MLXe twenty (20)-port 10-GbE/1-GbE (M) combo module with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules	Gen 3
BR-MLX-10Gx20-X2	20	MLXe twenty (20)-port 10-GbE/1-GbE (X2) combo module with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB. Requires high-speed switch fabric modules.	Gen 3
NI-MLX-10GX2	2	MLXe Series 2-port 10-GbE module with IPv4/IPv6/MPLS hardware support. Requires XFP optics.	Gen 1 [1]
NI-XMR-10GX2	2	XMR Series 2-port 10-Gbps Ethernet module. Requires XFP optics. IPv4, IPv6, MPLS support.	Gen 1 [1]
BR-MLX-100GX-1	1	MLXe/XMR/MLX 1-port 100-GbE (X) Module with IPv4/IPv6/MPLS hardware support - requires CFP optics. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode. Requires high speed switch fabric modules. License upgradable to 2-ports on an MLXe.	Gen 2
BR-MLX-100GX-2	2	MLXe 2-port 100-GbE (X) Module with IPv4/IPv6/MPLS hardware support - requires CFP optics. Supports 1M IPv4 routes in FIB in XMR mode and 512K IPv4 routes in MLX mode. Requires high speed switch fabric modules.	Gen 2
NI-MLX-10GX4	4	MLXe Series 4-port 10-GbE module with IPv4/IPv6/MPLS hardware support. Requires XFP optics.	Gen 1.1
NI-XMR-10GX4	4	XMR Series 4-port 10-GbE module with IPv4/IPv6/MPLS hardware support. Requires XFP optics.	Gen 1.1
BR-MLX-10GX4-X	4	XMR/MLX 4-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support. Requires XFP optics. Supports 1M IPv4 routes in FIB.	Gen 1.1
BR-MLX-10Gx4-X-ML	4	MLX 4-port 10-GbE (ML) module with IPv4/IPv6/MPLS hardware support. Requires XFP optics. Supports 512K IPv4 routes in FIB. License upgradable to "X" scalability (1M IPv4 routes in FIB).	Gen 1.1
BR-MLX-40Gx4-M	4	MLX 4-port 40-GbE (M) module with Layer 2, IPv4/IPv6, MPLS and OpenFlow support. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules and QSFP+ optics.	Gen 2
NI-MLX-10GX8-M	8	MLX Series 8-port 10-GbE (M) module with IPv4/IPv6/MPLS hardware support. Requires SFPP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules	Gen 2

TABLE 8 Interface modules for all MLX Series routers (continued)

SKU	Ports	Description	Generation
NI-MLX-10GX8-D	8	MLX Series 8-port 10-GbE (D) module with IPv4/IPv6 hardware support. Requires SFPP optics. Supports 256K IPv4 routes in FIB. Does not support MPLS. Requires high speed switch fabric modules	Gen 2
BR-MLX-10GX8-X	8	MLX/XMR 8-port 10-GbE (X) module with IPv4/IPv6/MPLS hardware support-requires SFPP optics. Supports 1M IPv4 routes in FIB. Requires high speed switch fabric modules.	Gen 2
NI-MLX-1GX20-SFP	20	MLX Series 20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support. Requires SFP optics. Note: Copper SFPs are supported at 1000Mbps only.	Gen 1 [1]
NI-XMR-1GX20-SFP	20	XMR Series 20-port FE/GE (100/1000) module with IPv4/IPv6/MPLS hardware support. Requires SFP optics. Note: Copper SFPs are supported at 1000Mbps only.	Gen 1 [1]
NI-MLX-1GX20-GC	20	MLX Series 20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.	Gen 1 [1]
NI-XMR-1Gx20-GC	20	XMR Series 20-port 10/100/1000 copper module with IPv4/IPv6/MPLS hardware support.	Gen 1 [1]
BR-MLX-1GCX24-X	24	XMR/MLX 24-port 10/100/1000 Copper (RJ-45) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	Gen 1.1
BR-MLX-1GCX24-X-ML	24	MLX 24-port 10/100/1000 Copper (RJ-45) Module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB. License Upgradable to "X" scalability (1M IPv4 routes in FIB).	Gen 1.1
BR-MLX-1GFX24-X	24	XMR/MLX 24-port 1-GbE Fiber (SFP) Module with IPv4/IPv6/MPLS hardware support. Supports 1M IPv4 routes in FIB.	Gen 1.1
BR-MLX-1GFX24-X-ML	24	MLX 24-port 1-GbE Fiber (SFP) Module with IPv4/IPv6/MPLS hardware support. Supports 512K IPv4 routes in FIB. License Upgradable to "X" scalability (1M IPv4 routes in FIB).	Gen 1.1
BR-MLX-10GX24-DM	24	MLX 24-port 10-GbE Module with IPv4/IPv6/MPLS hardware support - requires SFPP optics. Bandwidth up to 200Gbps per module. Supports 256K IPv4 routes.	Gen 1.1
NI-MLX-1GX48-T-A	48	MLX Series 48-port 10/100/1000Base-T, MRJ21 module with IPv4/IPv6/MPLS hardware support. Requires high speed fans NIBI-16-FAN-EXH-A on MLX-16.	Gen 1.1
[1] Support is discontinued for Gen 1 cards (20x1G all flavors; 4x10G all flavors except 4x10-X; and 2x10G all flavors).			

Depending on your router model, you can install up to 32 single-slot interface modules, or 16 double-slot interface modules.

Interface modules are hot-swappable, which means you can remove and replace them without powering down the system.

NOTE

Specific information regarding RAD optics configuration on the MLX Series platforms has been documented in the RAD optics Solutions test report. Please work with your account team to gain access to the document.

2x100GbE CFP2 optics based high density module

The 100GbE 2-port CFP2 optics based high density blade is a half slot module card for the MLX Series chassis.

The 2x100GbE CFP2 interface module is supported on all MLX Series routers.

> **NOTE**
> The 100G CFP2 ER4 optic is supported on this card for hardware revision 15 or later only. To check the version of the line card, enter the **show version slot** *slot-number* command. The version number must be 15 or later. The following example shows the version as version 15 in the underlined command output.

```
 MLX#show version slot 4
SL 4: BR-MLX-100Gx2-CFP2 2-port 100GbE Module
(Serial #: CWC0440K027, Part #: 60-1002934-15)
=====================================================
```

The 2x100GbE CFP2 based high density blade has the following features:

- 2x100GbE CFP2 optics half-slot ports
- 4GB DDR3 SDRAM (800MB Data Rate)
- 512K Flash Memory 2x16MB Code, 4MB Boot
- 64MB Flash Memory for Application Code
- PCI bus interface (PBIF) FPGA for PCIe Interface and STATS
- Hot Pluggable
- Power Consumption: 360W
- XPP FPGA for packet processing
- Temperature sensor, strategically located on the PCBA
- Power, port, and status LED indicators
- Link Status per port
- JTAG support
- Temperature monitoring I^2C Management Interface
- Real Time Clock
- Supports 32 GPIO
- Supports 9 temperature sensors

The 2x100GbE CFP2 based high density blade provides the following support:

- Extended VLAN statistics, sFlow monitoring, Optical Monitoring, CAM MIB, entity MIB, snAgentCpuUtilTable and system MIBs.
- snAgentConfigModuleTable, snSwIfInfoTable, snAgentBrdTable and brcdEntityOIDMIB.
- NP and TM counters and statistics.
- LP-Auto Upgrade.
- 4GB DDR3 SDRAM.

> **NOTE**
> Web Management Front Panel is not supported for the 2x100GbE CFP2 card.

> **NOTE**
> For NetIron 5.7 release only: 2GB of SDRAM memory is usable out of 4GB.

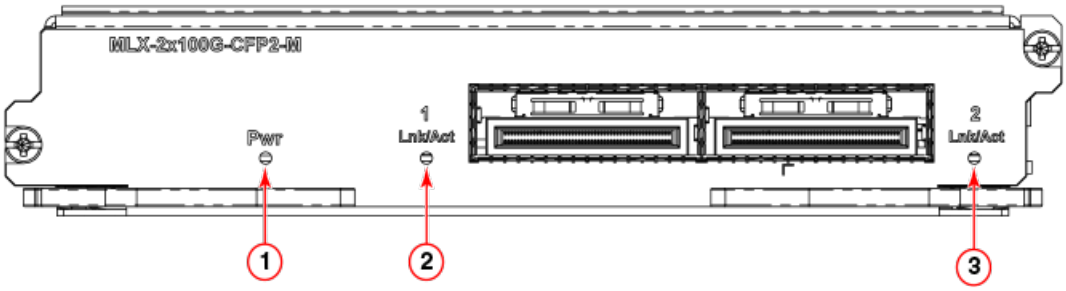
Traffic Manager (TM) traffic behavior for the 2x100GbE CFP2 card is as follows:

- E-Chassis and hSFMs are required with the 2x100GbE CFP2 module.

- Each 2x100GbE CFP2 TM can support one full 100Gbps wire speed ports.
- For best performance, Turbo mode is recommended; 1024B credit size; and full fabric connectivity.
- Performance in Turbo mode:
  - Line-rate with all SFMs installed except for some small packet sizes
  - No line-rate without all SFMs installed.
- Performance in non Turbo mode:
  - No line-rate even with all SFMs installed.

NOTE
Dynamic port configuration for the 2x100GbE CFP2 based high density blade chassis is shown in the topic 2x100GbE CFP2 Dynamic Port Configuration on page 275.

FIGURE 7 2x100GbE CFP2 interface module front panel



1. Pwr LED - if green: All power rails are functional and module is receiving power. If not lit (off): One or more power rails have failed and module is not receiving power.
2. 1 Link/Act LED: If green: CFP2 port 1 is functional. If not lit (off): CFP2 port 1 is not active.
3. 2 Link/Act LED: If green: CFP2 port 2 is functional. If not lit (off): CFP2 port 2 is not active.

2x100GbE CFP2 LED indicators and chassis support tables

LED indicators for the 2x100GbE CFP2 based high density blade indicate the status of each port, as described in the following table.

TABLE 9 2x100GbE CFP2 LED Indicators

LED Function/state	Location	Meaning	Possible cause
Power module state (LED) Controlled by the downloader FPGA; this LED is hardware controlled and is not software accessible.	Left side of module	GREEN: All power rails are functional and module is receiving power.	Power rails are enabled.
		OFF: One or more power rails have failed and module is not receiving power.	Power rails are disabled.
Link/Act	Adjacent to each port.	GREEN: All ports are functional.	Port is enabled and link is up.
		OFF: One or more ports have failed.	Port is disabled.

Chassis support for the 2x100GbE CFP2 based high density blade is shown in the following table.

TABLE 10 2x100GbE CFP2 Chassis Support

Ports	Chassis Supported	Description
2x100GbE CFP2	MLX Series	Support in MLX Series. **NOTE** XMR not supported.

CFP2 optics for 2x100GbE

The 2x100GbE CFP2 interface module is 802.3ba compliant, supports CFP2-based optics, and can be used with existing MLX Series interface modules. The 2x100GbE interface module requires high-speed fabric modules.

> **NOTE**
> 2x100GbE CFP2 interface modules will boot in turbo mode if all modules in the chassis are Gen-2 modules.

You must insert CFP2-compliant fiber-optic transceivers in each port you intend to use. CFP2-compliant transceivers provide an optical or physical medium-dependent (PMD) interface for single- or multi-mode fiber that can be used with either the LAN physical layer (PHY) or WAN physical layer (WAN PHY).

For a list of supported 2x100GbE CFP2-compliant fiber-optic transceivers that are available from Extreme Networks, refer to the latest version of the *Extreme Optics Family Data Sheet*.

For more information about fiber-optic transceivers and associated cabling, refer to Installing a fiber-optic transceiver on page 197.

Power supply requirements for 2x100GbE modules

For power supply requirements for the 2x100GbE modules, refer to Hardware Specifications on page 271.

PBIF Recovery

In the event PBIF gets locked up, PBIF recovery is activated by default with the option to activate PBIF recovery through the **system-monitoring pbif lp-reset-recovery** command.

Syntax

system-monitoring pbif lp-reset-recovery

no system-monitoring pbif lp-reset-recovery

Command Default

PBIF is locked up.

Examples

In the event PBIF is locked up, PBIF recovery is activated by default. However, if necessary you may activate PBIF recovery through the **system-monitoring pbif lp-reset-recovery** command.

```
device# config
device(config)# system-monitoring pbif lp-reset-recovery
device(config)# exit
device# write memory
device# reload
```

To deactivate PBIF recovery perform the **no system-monitoring pbif lp-reset-recovery** command.

```
device# config
device(config)# no system-monitoring pbif lp-reset-recovery
device(config)# exit
device# write memory
device# reload
```

History

Release version	Command history
5.7.00	This command was introduced.

2x100GbE CFP2 P2010 specifications

P2010 specifications are shown for the 2x100GbE CFP2 optics based high density blade.

TABLE 11 2x100GbE CFP2 P2010 Specifications

Component	Gen 2 Cards	2x100GbE CFP2 Cards
Processor	MPC8548E	P2010
Processor Version	0x8021_0022	0x8021_1051
System Version	0x8031_0021	0x80e3_0021
Core Version	E500V2	E500V2
Clock Speed	1.3GHz	1.2Ghz
Cache Support	32KB L1 instruction cache 32KB L1 data cache	32KB L1 instruction cache 32KB L1 data cache

TABLE 11 2x100GbE CFP2 P2010 Specifications (continued)

Component	Gen 2 Cards	2x100GbE CFP2 Cards
	512KB L2 cache	512KB L2 cache
Security Engine	Yes	Yes, enhanced SEC2 Interface
DDR Support	DDR/DDR2	DDR2/DDR3

2x100GbE CFP2 DDR3 SDRAM memory specifications

DDR3 SDRAM memory for the 2x100GbE CFP2 optics based high density blade, is shown in the following table.

TABLE 12 2x100GbE CFP2 DDR3 SDRAM Memory Specifications

Feature	Gen 2 Cards	2x100GbE Cards
DDR type	DDR2	DDR3
DDR size	2 GB	4GB **NOTE** For Extreme NetIron software 5.7 release only: 2GB of SDRAM memory is usable out of 4GB.
Data rate	Up to 533 Mbps	Up to 800 Mbps

BR-MLX-10GX20-X2 and BR-MLX-100GX2-CFP2-X2 Router Software

BR-MLX-10GX20-X2 and BR-MLX-100GX2-CFP2-X2 scalability for IPv4 and IPv6 routes

In Extreme NetIron software release 5.8.00a, the maximum number of routes supported with the BR-MLX-10GX20-X2 and BR-MLX-100GX2-CFP2-X2 modules has been scaled to 2.4M for IPv4 and 1.8M for IPv6. The -X2 scaling software is compatible with both MR2-M and MR2-X management modules so that you can deploy M, X, and -X2 modules in the same device.

NOTE
MR2 management modules require High Speed Switch Fabric modules.

show cam-partition usage

The **show cam-partition usage** command displays the CAM partition usage. IP CAM region is divided into partition and sub-partitions, with the super netting feature managing entries within these partitions and sub-partitions to achieve LPM (longest prefix match). Entries are shuffled across the sub-partition based on prefix length.

Syntax

show cam-partition usage

Examples

```
device#sh cam-partition usage

CAM partitioning profile: multi-service-3

XPP44GEX 0:
  [IPV6 Session]   8192(size),    8192(free),   0. 0%(used)
  :IPv6 Multicast:   2048(size),    2048(free),   0. 0%(used)
   :Receive ACL:      0(size),       0(free),   0. 0%(used)
      :Rule ACL:   6144(size),    6144(free),   0. 0%(used)

       [Session]  32768(size),   32767(free),   0. 0%(used)
  :IP Source Guard Denial:      0(size),       0(free),   0. 0%(used)
  :IP Source Guard Permit:      0(size),       0(free),   0. 0%(used)
          :Rule-based ACL:  23552(size),   23552(free),   0. 0%(used)
           :Broadcast ACL:      0(size),       0(free),   0. 0%(used)
             :Receive ACL:   1024(size),    1023(free),   0. 9%(used)
            :IP Multicast:   8192(size),    8192(free),   0. 0%(used)
         :IP Multicast 1G:      0(size),       0(free),   0. 0%(used)
        :IP Multicast 2GM:      0(size),       0(free),   0. 0%(used)
      :Open Flow CatchAll:      0(size),       0(free),   0. 0%(used)
   :Open Flow UnProtected:      0(size),       0(free),   0. 0%(used)
        :Open Flow Normal:      0(size),       0(free),   0. 0%(used)
     :Open Flow Protected:      0(size),       0(free),   0. 0%(used)

           [MAC] 131072(size),  131067(free),   0. 0%(used)
      :Protocol:     10(size),       5(free),  50. 0%(used)
    :Forwarding: 131024(size),  131024(free),   0. 0%(used)
      :Flooding:      8(size),       8(free),   0. 0%(used)
   :Port BUM RL:     30(size),      30(free),   0. 0%(used)

   [Out Session]  32768(size),   32768(free),   0. 0%(used)

[Out V6 Session]   8192(size),    8192(free),   0. 0%(used)

[Internal Forwarding Lookup] 131072(size),  131072(free),   0. 0%(used)
                  :IFL Main: 131062(size),  131062(free),   0. 0%(used)
     :IFL Openflow CatchAll:     10(size),      10(free),   0. 0%(used)

        [IP VPN] 196608(size),  196608(free),   0. 0%(used)

            [IP] 262144(size),  262123(free),   0. 0%(used)

          [IPV6]  65536(size),   65534(free),   0. 0%(used)
      [IPV6 VPN] 131072(size),  131068(free),   0. 0%(used)
```

History

Release version	Command history
NetIron R05.8.00	This command was introduced.

MLX Series 2x100G XPP ILKN monitoring

The 2x100G XPP ILKN monitoring feature will monitor CRC errors in the Interlaken link / interface between XPP1 and XPP2 in 2 packet processors for the 2x100G Ibzian card.

In 2x100G cards, CRC errors on the Interlaken link between iXPP1 and iXPP2 in the packet processor result in packet drops. The 2x100G XPP ILKN monitoring feature will generate syslog and SNMP traps if software reads more than configured drops on ILKN links between iXPP1 and iXPP2. Syslog and SNMP traps display the number of packet drops in the Interlaken interface and CRC errors in lane groups.

Two 100G ports are available. For each port:

- One XPP (with two internal ingress XPPs, iXPP1, iXPP2, and an egress XPP) is present to perform packet processing. This feature polls for Interlaken errors between ingress XPPs, iXPP1, and iXPP2.
- Two identical CXPP1x100G packet processors are present to perform 200Gbps packet processing.

SYSLOG and SNMP traps are generated if packet drops result from CRC errors in the Interlaken link / interface between iXPP1 and iXPP2. The affected ports are shutdown if the Interlaken link / interface was configured through the new CLI configuration command based on the following factors:

- The option to shutdown the affected ports is configured using the new global configuration command.
- The option to disable the feature is configured using the new global configuration command.

Syslog and SNMP traps are generated once the packets drop are seen because of Interlaken CRC errors. The syslog/SNMP trap is generated once every 3 minutes with the following information:

- Indicating the number of packet drops and CRC errors in each lane group.
- Indicating if ports are not disabled by the port shut down option.

MLX Series sysmon np interlaken-monitor

The global configuration command **sysmon np interlaken-monitor** {*crc-port-shutdown* | *disable*} is used to shut down available 100G ports if drops in the ILKN interface are more than the configured number of drops (*crc-port-shutdown*); or disable the feature (*disable*).

Syntax

sysmon np interlaken-monitor crc-port-shutdown

no sysmon np interlaken-monitor crc-port-shutdown

sysmon np interlaken-monitor disable

no sysmon np interlaken-monitor disable

Command Default

By default, the feature is enabled to poll ILK2 DROP COUNT register 0x200f4 every 30 seconds, and if there are 10 drops or more on ILK2 DROP COUNT register 0x200f4, then syslog and SNMP traps are generated.

Parameters

crc-port-shutdown

Port shutdown option is set globally for all the 2x100G cards available in the MLX Series device. The *crc-port-shutdown* global configuration command will be used to shut down the available 100G ports if the drops in ILKN interface are more than the configured number of drops. (**No** command is available to disable the port shutdown option.)

disable

Interlaken monitoring feature is disabled globally for all the 2x100G cards available in the MLX Series device. The *disable* global configuration command will be used to disable the feature. This command will be used disable the feature in all LP's across resets. (**No** command is available to enable the Interlaken monitoring option for all the 2x100 LPs available in the MLX Series device.)

Examples

The port shutdown option is set.

```
device(config)#sysmon np interlaken-monitor crc-port-shutdown
```

The Interlaken monitoring feature is disabled in all LPs.

```
device(config)#sysmon np interlaken-monitor disable
```

The **show interface Ethernet <slot/port>** CLI command will display the reason for port down as Interlaken CRC error.

```
device(config)#show int e 1/1
100GigabitEthernet1/1 is down(interlaken crc error), line protocol is down
  STP Root Guard is disabled, STP BPDU Guard is disabled
  NP transmitted 0 packets, Received from TM 0 packets
```

The **show sysmon config** CLI command will display the configuration details for ILKN CRC monitoring. Action is none by default. If **sysmon np Interlaken-monitor crc-port-shutdown** is configured, action will be displayed as DISABLE-PORTS. Mode will be displayed as POLLING by default and if the feature is disabled, then it will displayed as DISABLED. Poll period will display the value as 30 seconds, which is the global default configuration for this feature.

```
device(config)#show sysmon config
------------------------+-------+-------------------------+----------+-----------+------------
+-----------------+--------------------
EVENT            |ACTION|SLOTS                    |MODE      |POLL PERIOD| THRESHOLD  |LOGBACK-OFF
                       |            |                                  |                |
(SEC)           | #(PER POLL |
                       |            |                                  |                |  in
#POLL)      |                       |
------------------------+--------+-------------------------+-------------+-------------------
+-------------------+--------------------
NP ILKN          |NONE    | BR-MLX-100Gx2   |POLLING  |     30              |     N/A             |  N/A
Monitoring
```

History

Release version	Command history
Extreme NetIron Software Release 5.8.00	These commands were introduced.

MLX Series CPU threshold monitoring

CPU threshold monitoring generates a syslog when the hold time of any task exceeds the configured threshold time, for the purpose of troubleshooting to discover the reason for a CPU high condition (if applicable).

On encountering a high CPU condition, the resulting command output is not captured to determine the application that resulted in a high CPU condition. In many instances, the system recovers from high CPU conditions on its own. Syslog is a mechanism which can log tasks that cause high CPU conditions.

Syslog is generated when the hold time of any task exceeds the configured threshold time in active MP and LPs. Throttling allows the syslog to display the number of occurrences of high CPU conditions for a particular task in 5 minute intervals. Additional considerations include the following:

- This feature is enabled by configuring the **sysmon task-threshold** *time* global configuration command and is not available by default.
- The threshold time is configured using the **sysmon task-threshold** *time* global configuration command for active MP and all LPs, and is available across resets. The range of user configured threshold time is from 20ms to 1000ms. Default value recommended is 60ms.

MLX Series CPU Threshold Monitoring sysmon task-threshold

The threshold time is configured using the global configuration command `sysmon task-threshold <time>` for the active MP and all LPs, and will be available across resets.

Syntax

sysmon task-threshold *time*

no sysmon task-threshold *time*

Used to unconfigure the threshold value.

Parameters

time

Sets the **threshold-time** in milliseconds.

Modes

Global configuration

Examples

The following configuration example configures the `task-threshold` to default 60ms:

```
device(config)#sysmon task-threshold 60
Task threshold-time is set to default value 60ms.
```

The following configuration example sets the `task-threshold` to 50ms:

```
device(config)#sysmon task-threshold 50
Task threshold-time is set to 50ms.
```

When hold time exceeds the configured threshold, i.e. 20ms for sfm_mgr task, the below syslog gets generated:

```
Nov 26 14:12:11:I:System: High CPU condition on MP, task name=sfm_mgr, max hold time=29ms, count =11
Nov 26 14:07:11:I:System: High CPU condition on MP, task name=sfm_mgr, max hold time=29ms, count =1
```

History

Release version	Command history
Extreme NetIron software R05.8.00	This command was introduced.

MLX Series BR-MLX-10Gx4-M IPsec and IKEv2

The MLX Series router is located on the perimeter of connections to external networks. Encryption and decryption is supported for IPv4 unicast data and control packets transmitted or received from external networks, using IPSec FPGA and IKEv2 protocols for the MLX Series BR-MLX-10Gx4-M-IPSEC.

The Public Key Infrastructure (PKI) provides a security infrastructure for secure communication. Each PKI peer holds a Digital Certificate which holds multiple attributes that ensure the entity can be trusted, and can support secure communication.

- IPSec FPGA protocol for the MLX Series BR-MLX-10Gx4-M-IPSEC provides hardware based data encryption and decryption.
- IKEv2 protocol for the MLX Series BR-MLX-10Gx4-M-IPSEC is used to setup and manage secure tunnels across external networks.

PKI uses the asymmetric encryption algorithm; two different keys are used to encrypt and decrypt data. The key pair consists of a private key and a public key. The private key must be kept secret, while the public key can be distributed. Data encrypted by one of the two keys can only be decrypted by the other. Data encrypted with a public key cannot be decrypted using a public key and vice versa. Users of a public key are confident that the associated private key is owned by the correct remote subject.

MLX Series Encryption and Decryption of IPv4 Unicast Data and Control Packets

Features include for encryption and decryption of IPv4 unicast data and control packets include IKEv2 on MP; IPSec FPGA protocol; IKEv2 protocol support; and PKI checks for certificate presence.

Major enhancements to support encryption and decryption of IPv4 unicast data and control packets transmitted or received from external networks include:

- IPSec FPGA protocol using a new 4x10G/1G and 4x1G IPSec line card, developed to provide hardware based data encryption and decryption at line rate of 44GBe. This card has free scale P2010 CPU with Security Engine 3.1x.
- IKEv2 protocol support to setup and manage secure tunnels across the external network.
- PKI support for authentication of endpoints of tunnel using digital certificates.

  NOTE
  The PKI module needs to run over HTTP, so it will be running as a separate task on MP.
  IKE or another module should not store the PKI certificates for later reference. Whenever needed, the PKI module should be queried with the certificate DN or Subject's alternate name.

- Manual PKI is supported, and OCSP and SCEP are not supported (for Extreme NetIron Software Release 5.8.00).

MLX Series IKEv2 Authentication

When IKEv2 authentication is configured and the method (remote or local) is ECDSA, the CA certificates are retrieved and downloaded to LPs where IKE will store these certificates. This is done even if the peer is not up, such as during peer init. This data is required or **SA-INIT** cannot be completed.

NOTE
The new PKI feature in the Extreme NI Release 5.8.00 will only be used for setting up the IKEv2 session.

When a peer is created and auth method is ECDSA IKE checks its database to ascertain if the CA and its self certificate are available.

The following certificate payload encoding is supported:

Certificate Type	Value
X.509 Certificate – Signature	4
Hash and URL of X.509 certificate	12
OCSP content	14

During the IKEv2 exchange, when two peers are establishing a tunnel, each peer will receive a certificate from the other IKE peer. In the IKE, the certificates can be sent in two ways: Inline certificate and HTTP and URL format.

NOTE
IKE or another module should not store the PKI certificates for later reference. Whenever needed, the PKI module should be queried with the certificate DN or Subject alternate name.

MLX Series IPsec and IKEv2 configuration

Create a VTI interface by creating a tunnel interface and setting the mode of the tunnel to IPsec IPv4.

To create a tunnel interface and set the mode of the tunnel to IPsec IPv4, perform the following task.

1. Create a VTI interface by completing the following steps:
   a) Create a VTI interface by entering the **interface tunnel** *x* command, where *x* is the tunnel number.
   b) Set the mode of the tunnel to IPsec IPv4 by entering the **tunnel mode ipsec ipv4**command.
2. Configure the following values, if the default values are not acceptable.
   - IKE Proposal
   - IKE Policy
   - IKE Profile
   - IKE Authentication
   - IPSEC Proposal
   - IPSEC Profile
3. Bind the IPsec Profile to the VTI interface using the **tunnel protection ipsec profile** *profilename* command.

MLX Series Configuring Global IKEv2 Options

Configure global IKEv2 options that are independent of peers. All the global IKE commands start with prefix **ikev2**.

IKEv2 Option	Description
ikev2 retry-count *<number>*	Maximum number of attempts to retransmit a message. Default 5. NOTE Range is 1 to 10.
ikev2 exchange-max-time *<seconds>*	Maximum setup time for an exchange, in seconds. Default 30 seconds. NOTE Range is 0 to 300 seconds.
ikev2 retransmit-interval *<time>*	IKEv2 message resend delay, in seconds. This is the time that the IKEv2 task is to wait before attempting the first resend of a packet. Default is 5 seconds. Retransmit interval will increase exponentially. NOTE Range is 1 to 60 seconds.
ikev2 http-url-cert	Enables the HTTP CERT support. HTTP CERT is disabled by default. If enabled then HTTP_CERT_LOOKUP_SUPPORTED should be send along with the CERT_REQ payload. Default is disabled.
ikev2 cookie-challenge *<number >*	Enabled an IKEv2 cookie challenge only when the number of half-open IKE SAs crosses the configured number. Default is disabled. NOTE Range is 1 to 2000 (max number of SA supported).
ikev2 limit { max-in-negotiation-sa limit | max - sa limit }	max-in-negotiation-sa limit — Limits the total number of in negotiation IKEv2 SAs on the node. Default is 256. max-sa limit — Limits the total number of IKEv2 SAs on the LP. Default is 256. NOTE For both limits the range is 1 to 256 (max SAs supported).
ikev2 Allow duplicate ike-sa	For a given source/destination and IKE Profile, if multiple IKE SA can be created. This will be applicable only for incoming IKE session. Default is disabled. This will be used for inter-op with other vendors.

IKEv2 Option	Description
	NOTE Not supported for NI R05.8.00 release.
ikev2 fragmentation [mtu-size]	(Optional) To support fragmentation of IKEv2 message into small parts to avoid UDP level fragmentation. Default it is disabled. It is at the global level because the routing can change, and we should be able to estimate what will be the maximum size for the router. Range should be between 68 to 1500. **NOTE** Not supported for Extreme NetIron software R05.8.00 release.

MLX Series Configuring the IKEv2 Proposal

IKEv2 Proposal sets the configurable parameters which are exchange during IKEv2 peer negotiation during the first phase.

The default IKEv2 proposal requires no configuration and its parameters are as follows:

- Encryption: aes-cbc-256
- PRF: sha384
- Integrity: sha384
- dh-group: 20

This default IKEv2 proposal will be known as **ikev2-default-proposal**.

The following commands are available to configure the proposals manually, if you do not want to use the default proposal.

NOTE
The default proposal command will only be available if additional cryptographic algorithms are supported, as currently there is no requirement to support them in Extreme NetIron software Release 5.8.00.

IKEv2 Option	Description
ikev2 proposal *<name>*	Configure IKE proposal Parameter, enter **ikev2 proposal** *<name>* config mode.
dhgroup {1} {2} {5} {14} {15} {16} {19} {20} {24}	Group used for Diffie-Hellman negotiations. Allowed values are: • 1 — 768-bit DH • 2 — 1024-bit DH • 5 — 1536-bit DH • 14 — Specifies the 2048-bit DH group. • 15 — Specifies the 3072-bit DH group. • 16 — Specifies the 4096-bit DH group. • 19 — Specifies the 256-bit elliptic curve DH (ECDH) group. • 20 — Specifies the 384-bit ECDH group. • 24 — Specifies the 2048-bit DH/SA group. **NOTE** For the first release, only DH-group 14, 19, and 20 will be supported. Support for other DH groups will be considered for inclusion in the next major release.
prf { sha384 | sha256 }	Hash algorithm to be used to generate key material for IKE SA negotiation. Multiple algorithms may be specified, separated by commas.
encryption {3des} {aes-cbc-128} {aes-cbc-192} {aes-cbc-256}	Encryption algorithm to be used to protect IKEv2 data. Multiple algorithms may be specified. Allowed values are: • 3des • aes-cbc-128 • aes-cbc-192

IKEv2 Option	Description
	• aes-cbc-256 **NOTE** For the first release, only aes-cbc-128 and aes-cbc-256 will be supported. Support for other encryption for IKEv2 will be considered for inclusion in the next major release.
integrity {sha1} {sha256} {sha384} {sha512}	Integrity algorithm to be used to protect IKEv2 data. Multiple algorithms may be specified. The following are supported: • sha1 — specifies SHA-1 (HMAC variant) as the hash algorithm. • sha256 — specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm. • sha384 — specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm. • sha512 — specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm. **NOTE** For the first release, only sha256 and sha384 will be supported. Support for other crypto for IKEv2 will be considered for inclusion in the next major release.

MLX Series Configuring the IKEv2 Policy

After you create the IKEv2 proposal, the proposal must be attached to a policy to pick the proposal for negotiation.

The IKE policy states which security parameters will be used to protect IKE negotiations. An IKEv2 policy must contain at least one proposal to be considered as complete. It can have local-address and VRF statements which are used as selection criteria to select a policy for negotiation. During the initial exchange, the local address and the VRF of the negotiating SA are matched with the policy and the proposal is selected.

There will be a default IKEv2 policy named **ikev2-default-policy** and it will have the following parameters:

- Proposal: ikev2-default-proposal
- local_address: not set, match all local addresses
- VRF: not set so will match any-vrf

If no suitable IKE policy is found, the IKE session will be established using the **ikev2-default-policy**.

For a given local ip-address only one policy can be chosen.

Configuration of overlapping policies is considered a misconfiguration. In the case of multiple, possible policy matches, the first policy is selected.

IKEv2 Option	Description
ikev2 policy *<name>*	Configure IKE policy parameters, enter ikev2 policy configuration mode.
Proposal *<name>*	Specify at least one proposal; optionally, you can specify additional proposals. This is only for IKE SA.
match address-local *<ipaddress> <mask>*	(Optional) Matches the policy based on the local IPv4. If not configured, it will match all the local IPv4 addresses.
match fvrf { vrf-name *<name>* | any }	(Optional) The FVRF in which the local IP address on the IKEv2 packet should be matched. If not configured, it will match the any-vrf.

MLX Series Configuring the IKEv2 Profile

An IKE profile is used in phase two of an initial exchange to determine the authentication profile to be applied for an incoming IKE session. During a session, it also determines the choice of local identifier.

An IKE session has the following criteria:

- Unique IKE profile, set of local-IP address, and remote-IP address.
- Applies parameters to an incoming IPsec connection that is uniquely identified through its match identity criteria.

These IKE profile criteria are based on the IKE identity that is presented by incoming IKE connections, and includes the IP address, fully qualified domain name (FQDN), and other identities. Once the IKE profile is chosen, it can be used to protect single or all VRF.

For an outgoing connection, the IKE profile is chosen based on the IPsec-Profile used by VTI. The IKE policy will be selected based on the local IP-address.

The following rules apply to match statements:

- An IKEv2 profile must contain an identity to match; otherwise, the profile is considered incomplete and is not used. An IKEv2 profile can have more than one match identity.
- An IKEv2 VRF will match with the VTI Base VRF.
- When a profile is selected, multiple match statements of the same type are logically ORed, and multiple match statements of different types are logically ANDed.
- Configuration of overlapping profiles is considered a misconfiguration. In the case of multiple profile matches, the first profile will be selected.

IKEv2 Option	Description
Ikev2 profile *<name>*	Defines an IKEv2 profile name and enters IKEv2 profile configuration mode.
description *<description>*	(Optional) Description text for this profile.
authentication *<authentication-proposal -name>*	Authentication Proposal to be used with this IKE profile.
local_identifier { address *<ipv4-address>*dn | dn *<dn-string>* | fqdn *<fqdn-string>* | key-id *<key-id String>* | email *<email-string>* }	(Optional) Local system ID to be sent with ID payload during negotiation. Allowed formats of this entry are as follows: • address is IPv4. • dn is Distinguished name. • FQDN is Fully Qualified Domain Name. For example, router1.example.com. • email is E-mail ID. For example,test@test.com. • key-id is Key ID.
remote-identifier { address *<ipv4-address>*dn | dn *<dn-string>* | fqdn *<fqdn-string>* | key-id *<key-id String>* | email *<email-string>* }	(Optional) Remote system ID that we want to communicate with. Allowed formats of this entry are as follows: • address is IPv4. • dn is Distinguished name. • FQDN is Fully Qualified Domain Name. For example, router1.example.com. • email is E-mail ID. For example,test@test.com. • key-id is Key ID.
keepalive *<seconds>*	(Optional) Interval, in seconds, between the IKE Notify messages sent to query peer liveness and thus detect a dead peer. Default is enabled and the default value is 30 sec. Range should be between 0-3600 seconds. 0 means that keep-alive is not enabled.
lifetime *<minutes>*	(Optional) IKE SA lifetime in minutes. Default is 24 Hours, 1440 minutes. Range should be between 10-1440 minutes.
responder-only	(Optional) In responder-only mode, this host acts as the responder and does not initiate negotiation and rekeying. Otherwise, this host acts as initiator; negotiation starts when the IKE Peer is reachable. By default the router behave as both initiator and responder.

IKEv2 Option	Description
[no] initial-contact-payload	(Optional) This host may have rebooted and peers may have SAs that are no longer valid. Use the value on to send an initial contact message to a peer, so that it will delete old SAs. Use the value off to disable this feature. Default is disabled.
match identity { local { **address** { *<ipv4-address>* } } | dn *<dn-string>* | email *<email-string>* | fqdn *<fdqn-string>* | key-id *<key-id string>* | } remote { address { *<ipv4-address>* [mask] } | dn *<dn-string>* | email *<email-string>* | fqdn *<fdqn-string>* | key-id *<key-id string>* }	To Select IKE profile (PAD) for a peer based on local or remote received Identity parameters such as the IP address, email or FDQN.
Protected *<vrf>*	The VRF traffic to protect using IPsec. If the tunnel VRF and protected VRF does not match, the IKE session is not initiated. Change to this parameter is not allowed if the profile is already in use by a tunnel. (Default value is any VRF.)

MLX Series Configuring the IKEv2 authentication proposal

IKEV2 peers must be authenticated for their identity. Local IKE connections need to send a local-identity to peers for authentication. All required authentication parameters for local and remote peers can be configured inside this authentication template. This authentication template can be used with multiple IKE profiles.

An authentication proposal should be mapped to an IKE Profile. Once a suitable IKE profile is selected for an incoming IKE session, the authentication proposal will be used the verify the AUTH data.

If a received authentication method is not specified in this proposal, the authentication is assumed to have failed, and necessary action is taken accordingly.

IKEv2 Option	Description
Ikev2 auth-proposal *<auth-name>*	Defines an IKEv2 authentication name and enters authentication configuration mode.
method { **local** {ecdsa384 | pre-shared} | **remote** {ecdsa384 | pre-shared} }	Authentication method. Allowed values are pre_shared_key, rsa_signature, dss_signature. Multiple methods may be specified for remote authentication (not applicable for first release). Only one method is allowed for local authentication. Only x509v3certificate with digital signature using ecdsa384 will be supported for first release.
pki trustpoint *<trustpoint-Name>* [sign | verify]	(Optional) Specifies the certificate authority (trustpoint) for use for signing and authentication of Auth payload. Different trustpoints can be used for signing and verification of Auth Payload. sign — Use the certificate from the trustpoint to sign the AUTH payload sent to the peer. verify — Use the certificate from the trustpoint to verify the AUTH payload received from the peer. NOTE Only ipv4 domain will be supported in first release. Ipv6 domains will be considered in future release.
pre-shared-key *<key>*	If the authentication method is used as pre-shared, then the pre-shared key should be configured. NOTE There is no default value for this parameter.

MLX Series Configuring the IPsec Proposal

Configure the IPsec proposal to specify the IPsec encryption parameters. The IPsec proposal contains the ESP and AH method to be used. This will be linked to an IPsec policy.

The default proposal **ipsec-default-proposal** is defined at IPsec initialization time with the following parameters:

- Authentication and encryption: esp- aes-gcm-256
- **transform** esp
- **encapsulation-mode** tunnel

IKEv2 Option	Description
ipsec proposal *<name>*	Defines an IPsec Security Proposal Name and enters IPsec proposal configuration mode.
encapsulation-mode {transport | tunnel}	The packet encapsulation mode is configured. By default, the security protocol uses the tunnel mode to encapsulate IP packets. NOTE In the first release, only tunnel mode will be supported.
encryption-algorithm {aes-gcm-256}	Configure the encryption algorithm to be supported. NOTE For the first release gcm-256 is supported.
transform {esp}	Configure transform to be used. For release 5.8.00 esp will be supported.
ESN-enable	Enable Extended Sequence Number in this transform. By default it is disabled. Use this command to enable it. NOTE The setting for this command must match the setting for replay-protection (for the IPsec profile).

MLX Series Configuring the IPsec Profile

The IPsec profile configuration defines the IPsec parameters to be used for encryption between IPsec routers.

For the IPSEC profile to be active and used for creating child-SA, the profile should be attached with a VTI interface. The profile should have an IPsec proposal defined; otherwise, it will use the default IPsec proposal.

NOTE
There is no support for manual IPsec key entry.

If there is no IKE peer (source, destination, and VRF of VTI), then attaching the IPsec profile to VTI should initiate a new IKE session (if the IKE profile is not configured as passive).

If there is already an IKE peer for the given source, destination, IKE profile and outgoing VRF, then a new child-SA should be created.

IKEv2 Option	Description
ipsec Profile *<name>*	Defines the IPsec parameters to be used between two IPsec routers, and enter IPsec configuration mode.
Description *<string>*	(Optional) Description text for this IPsec profile.
Ike-profile *<ike-profile-name>*	IKE profile attached with this IPsec profile.
Lifetime [minutes]	(Optional) Lifetime of the IPsec SA in minutes. By default it is 8 hours, 480 minutes. The new security association will be started 5 minutes before the old one is about to expire.

IKEv2 Option	Description
	NOTE Range of interval: 10 - 1440
Proposal *<proposal-name>*	The IPsec proposal to be used with this IPsec profile. Multiple proposals can be specified.
Replay-protection	(Optional) Disable anti-replay checking for a particular IPsec Profile. By default it is disabled. **NOTE** The setting of this command must match the setting of ESN-enable under the IPsec proposal.

MLX Series IKEv2 Show Commands

IKEv2 show commands include configured proposals, policy, profile, security associations, sessions, certificates, counters, security associations, statistics, proposals, and database for security policies.

IKEv2 Option	Description
Show ikev2 proposal [name]	Show configured IKEv2 proposals.
Show ikev2 policy [policy-name]	Show IKEv2 policy.
Show ikev2 profile [profile-name]	Show IKEv2 profile.
Show ikev2 sa [spi-index | fvrf *<vrf-name>* | local *<address>* | remote *<address>*] [detail]	Show IKEv2 security associations.
Show ikev2 {session [local-spi-id]} [detail]	Show IKEv2 sessions.
Show ikev2 certificate	Show certificates used by IKEv2.
Show ikev2 statistics	Show ikev2 counters.
Show ipsec profile [profile-name]	Show configured IPSEC profiles.
Show ipsec proposal [proposal-name]	Show configured IPSEC proposals.
Show ipsec sa [address *<address>* | identity *<id>* | interface *<name>* | peer address] [detail]	Show IPSEC security associations.
show ipsec statistics [tunnel *<tunnel-id>*]	Show Ipsec SA statistics.
Show ipsec Policy	Displays the database for the IPsec security policies.

Examples of Show Commands

show ikev2 proposal:

```
device# show ikev2 proposal

     Name       : ikev2-default-proposal
     Encryption : AES-CBC-256
     Integrity  : sha384
     PRF        : sha384
     DH Group   : 384_ECP/Group 20
```

show ikev2 policy:

```
device# show ikev2 policy

   Name                : ike_policy_red
   vrf                 : Default
```

```
  Local address/Mask  : 0.0.0.0/0.0.0.0
  Proposal            : ike_proposal_red

  Name                : ikev2-default-policy
  vrf                 : Default
  Proposal            : ikev2-default-proposal
```

show ikev2 profile:

```
device# show ikev2 profile

 IKEv2 profile       : ike_profile_blue
 Auth Profile        : auth_blue
 Match criteria      :
  IKE session vrf    : default-vrf
  Local:
   address 1.2.10.1
  Remote:
   address 1.2.10.2
 Local identifier    : address 1.2.10.1
 Remote identifier   : address 1.2.10.2
 Local auth method: pki
 Remote auth method(s): pki
 Lifetime          : 86400 sec
 keepalive check   : disabled


 IKEv2 profile     : ike_profile_green
 Auth Profile: auth_green
 Match criteria:
  IKE session vrf  : default-vrf
  Local:
   address 1.2.10.1
  Remote:
   address 1.2.10.2    fdqn RTB_green
 Local identifier  : address 1.2.10.1
 Remote identifier : address 1.2.10.2
 Local auth method: pki
 Remote auth method(s): pki
 Lifetime          : 1440 minutes
 keepalive check   : disabled
```

show ikev2 sa:

```
device# show ikev2 sa


tnl-id     local                 remote                Status      vrf(i) vrf(f)
-------------------------------------------------------------------------------
tnl 2      1.2.10.1/500          1.2.10.2/500          rdy  Blue   Default




device# show ikev2 sa detail

tnl-id     local                 remote                status      vrf(i) vrf(f)
-------------------------------------------------------------------------------
2          1.2.10.1/500          1.2.10.2/500          rdy  Blue   Default
      Role                : Initiator
      Local SPI           : 0xf327d32cd0df9106     Remote SPI: 0x34bec986ed6c232e
      Ike Profile         : mlx2_1
      Ike Policy          : mlx2_1
      Auth Proposal       : def-ike-auth-prop
```

show ikev2 session:

```
device# show ikev2 session

IKE count:1, CHILD count:1
```

```
Tunnel-id  Local                 Remote                Status      vrf(i) vrf(f)
-------------------------------------------------------------------------------
Tnl 2          1.2.10.1/500          1.2.10.2/500          rdy|in-use  Blue   Default
child sa:
 id 1
       local selector  0.0.0.0/0 - 255.255.255.255/65535
       remote selector 0.0.0.0/0 - 255.255.255.255/65535
       ESP spi in/out: 0x0000004b/0x0000005e
       Encryption: aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null
       Authentication: null  DH Group:none , Mode: tunnel



device# show ikev2 session detailed

IKE count:1, CHILD count:1

Tunnel-id  Local                 Remote                Status      vrf(p) vrf(f)
-------------------------------------------------------------------------------
2          1.2.10.1/500          1.2.10.2/500          rdy|in-use  Blue   Default
      Encr: aes-cbc-256, Hash: sha384, DH Grp:384_ECP/Group 20, Auth: not supported
    Life/Active Time: 86400/361 sec
    Status Description: Negotiation done
       Local spi: f7c029048eb25082       Remote spi: 56b8735e2f6afbde
       Local id : address 1.2.45.2       Remote id : address 1.2.45.1
       No Exchange in Progress
       Next Request Message id=29
          Total Keepalive sent: 0     Total Keepalive Received: 0
       Time Past Since Last Msg: 60

child sa:
 id 1
       local selector  0.0.0.0/0 - 255.255.255.255/65535
       remote selector 0.0.0.0/0 - 255.255.255.255/65535
       ESP spi in/out: 0x0000004b/0x0000005e
       Encryption: aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null
       Authentication: null  DH Group:none , Mode: tunnel
```

Show ipsec proposal:

```
device# Show ipsec proposal

   Name          : prop_red
   Protocol      : ESP
   Encryption    : aes-gcm-256
   Authentication: NULL
   ESN           : Enable
   Mode          : Tunnel
```

Show ipsec Profile:

```
device# Show ipsec Profile

Name                : red
Ike Profile         : red
Lifetime            : 28800
Anti-replay service : Enabled
 Replay window size : 64
DH group            : None
Proposal            : red
```

show ipsec sa:

```
device#show ipsec sa
             IPSEC Security Association Database(Entries:2)
SPDID(vrf:if) Dir Encap SPI        Destination
  AuthAlg  EncryptAlg Status Mode
0:v2          out ESP   400        ::
  sha1     Null       ACT    TRAN
0:v2          in  ESP   400        FE80::
  sha1     Null       ACT    TRAN
```

```
1:Tun1         in   ESP   0xBD481319   1.2.10.2
  Null      AES-GCM-256 ACT     TNL
1:Tun1         out  ESP   0x9EAB77D6   1.2.10.2
  Null      AES-GCM-256 ACT     TNL


device# Show ipsec sa address 1.2.10.2 detail
Total ipsec SAs: 2

0:
    interface           : tnl 1
     Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
     Inside vrf: default-vrf
     Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
     Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
     DF-bit: clear
     Profile-name: red
     DH group: none
     Direction: inbound, SPI: 0x0000004b
     Mode: tunnel,
     Protocol: esp, Encryption: gcm-256, Authentication: null
     ICV size: 16 bytes
     lifetime(sec): Expiring in (4606816/3576)
     Anti-replay service: Enabled, Replay window size: 0
     Status: ACTIVE
     slot Assigned 0
     nht_index 0000ffff
     Is tunnel NHT: false
1:
    interface           : tnl 1
     Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
     Inside vrf: default-vrf
     Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
     Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
     DF-bit: clear
     Profile-name: red
     DH group: none
     Direction: inbound, SPI: 0x0000009c
     Mode: tunnel,
     Protocol: esp, Encryption: gcm-256, Authentication: null
     ICV size: 16 bytes
     lifetime(k/sec): Expiring in (4606816/3576)
     Anti-replay service: Enabled, Replay window size: 0
     Status: ACTIVE
     slot Assigned 0
     nht_index 00000004
     Is tunnel NHT: true
```

show ipsec policy:

```
device#show ipsec policy
             IPSEC Security Policy Database(Entries:2)
PType  Dir Proto Source(Prefix:TCP/UDP Port)
                 Destination(Prefix:TCP/UDPPort)
  SA: SPDID(vrf:if) Dir Encap SPI        Destination
use    in  OSPF  FE80::/10:any
                 ::/0:any
  SA: 0:v2          in  ESP   400        FE80::

use    out OSPF  FE80::/10:any
                 ::/0:any
  SA: 0:v2          out ESP   400        ::
use    in  all    0.0.0.0/0:any
                  0.0.0.0/0:any
  SA: 1:Tun1         in   ESP  0xBD481319 1.2.10.2
use    out  all    0.0.0.0/0:any
                   0.0.0.0/0:any
  SA: 1:Tun1         out  ESP  0x9EAB77D6 1.2.10.2
```

show ipsec stat:

```
device#show ipsec stat
                        IPSecurity Statistics
ipsecEspCurrentInboundSAs 1          ipsecEspTotalInboundSAs:  1
ipsecEspCurrentOutboundSA 1          ipsecEspTotalOutboundSAs: 1
                      IPSecurity Packet Statistics
ipsecEspTotalInPkts:      0          ipsecEspTotalInPktsDrop:  0
ipsecEspTotalOutPkts:     7
                      IPSecurity Error Statistics
ipsecAuthenticationErrors 0
ipsecReplayErrors:        0          ipsecPolicyErrors:        0
ipsecOtherReceiveErrors:  0          ipsecSendErrors:          0
ipsecUnknownSpiErrors:    0
```

show ikev2 statistics:

```
device#show ikev2 statistics
Total IKEv2 SA Count   : 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0
Incoming IKEV2 Cookie Challenged Requests: 0
accepted: 0 rejected: 0 rejected no cookie: 0
IKEv2  Packet Statistics:
    Total Packets Received     : 57
    Total  Packets Transmitted : 57
    Total Packets Retransmitted: 0
    Total Keepalive Received   : 10
    Total Keepalive Transmitted: 10
IKEv2 Error Statistics:
    Unsupported Payload   : 0     Invalid IKE SPI  : 0
    Invalid Version       : 0     Invalid Syntax   : 0
    Proposal Mismatch     : 0     Invalid Selectors: 0
    Authentication Failed : 0     Others           : 0
```

MLX Series IKEv2 Clear Commands

IKEv2 **clear** commands include **clear ikev2 sa**, **clear ipsec statistics**, **clear ike statistics**, and **clear ipsec sa**.

IKEv2 Option	Description
clear ikev2 sa { fvrf *<vrf-name>* } { [local *<ipaddress>*] | [remote *<ip-address>*] }	Clear IKE security associations. When the user gives this command, the IKE SA will be deleted and re-established. Each child SA is also re-established.
clear ipsec statistics	Clears the IPsec statistics.
clear ike statistics	Clears all IKE related stats.
clear ipsec sa [fvrf *<vrf-name>*] [peer *<ip-address>*]	Clears IPsec SA. This command deletes and then creates the IPsec SA. The IKE SA will remain the same.

MLX-10GX4-IPSEC-M Forwarding

Card features for the MLX-10GX4-IPSEC-M include port to port line rate forwarding for all packet sizes, and line rate forwarding with combinations of 1G, 10G, 100G and 40G ports.

The MLX-10GX4-IPSEC-M card is designed for the MLX Series chassis, and its features include the following:

- CAM1 and CAM3 interface parallel look-ups.

  NOTE
  Transparent to MLX-10GX4-IPSEC-M forwarding application.

- P2010 free scale processor and security engine, with free scale processor running at 1.2Ghz; 4GB DDR3 SDRAM; 512K flash memory boot code; and 64MB flash memory for application code.
- 4x1GE SFP and 4x10GE SFP+ ports.
- Support for 6 temperature sensors and 32 GPIO.

  NOTE
  Long Term Repeat rate (LTR) exceeds fifty.

- Support for 4x10G SFM (only with HSFM), which results in LP entering an interactive state.

MLX Series 2x100G XPP ILKN monitoring

The 2x100G XPP ILKN monitoring feature will monitor CRC errors in the Interlaken link / interface between XPP1 and XPP2 in 2 packet processors for the 2x100G Ibzian card.

In 2x100G cards, CRC errors on the Interlaken link between iXPP1 and iXPP2 in the packet processor result in packet drops. The 2x100G XPP ILKN monitoring feature will generate syslog and SNMP traps if software reads more than configured drops on ILKN links between iXPP1 and iXPP2. Syslog and SNMP traps display the number of packet drops in the Interlaken interface and CRC errors in lane groups.

Two 100G ports are available. For each port:

- One XPP (with two internal ingress XPPs, iXPP1, iXPP2, and an egress XPP) is present to perform packet processing. This feature polls for Interlaken errors between ingress XPPs, iXPP1, and iXPP2.
- Two identical CXPP1x100G packet processors are present to perform 200Gbps packet processing.

SYSLOG and SNMP traps are generated if packet drops result from CRC errors in the Interlaken link / interface between iXPP1 and iXPP2. The affected ports are shutdown if the Interlaken link / interface was configured through the new CLI configuration command based on the following factors:

- The option to shutdown the affected ports is configured using the new global configuration command.
- The option to disable the feature is configured using the new global configuration command.

Syslog and SNMP traps are generated once the packets drop are seen because of Interlaken CRC errors. The syslog/SNMP trap is generated once every 3 minutes with the following information:

- Indicating the number of packet drops and CRC errors in each lane group.
- Indicating if ports are not disabled by the port shut down option.

MLX Series sysmon np interlaken-monitor

The global configuration command **sysmon np interlaken-monitor** {*crc-port-shutdown* | *disable*} is used to shut down available 100G ports if drops in the ILKN interface are more than the configured number of drops (*crc-port-shutdown*); or disable the feature (*disable*).

Syntax

sysmon np interlaken-monitor crc-port-shutdown

no sysmon np interlaken-monitor crc-port-shutdown

sysmon np interlaken-monitor disable

no sysmon np interlaken-monitor disable

Command Default

By default, the feature is enabled to poll ILK2 DROP COUNT register 0x200f4 every 30 seconds, and if there are 10 drops or more on ILK2 DROP COUNT register 0x200f4, then syslog and SNMP traps are generated.

Parameters

crc-port-shutdown

Port shutdown option is set globally for all the 2x100G cards available in the MLX Series device. The *crc-port-shutdown* global configuration command will be used to shut down the available 100G ports if the drops in ILKN interface are more than the configured number of drops. (**No** command is available to disable the port shutdown option.)

disable

Interlaken monitoring feature is disabled globally for all the 2x100G cards available in the MLX Series device. The *disable* global configuration command will be used to disable the feature. This command will be used disable the feature in all LP's across resets. (**No** command is available to enable the Interlaken monitoring option for all the 2x100 LPs available in the MLX Series device.)

Examples

The port shutdown option is set.

```
device(config)#sysmon np interlaken-monitor crc-port-shutdown
```

The Interlaken monitoring feature is disabled in all LPs.

```
device(config)#sysmon np interlaken-monitor disable
```

The **show interface Ethernet <slot/port>** CLI command will display the reason for port down as Interlaken CRC error.

```
device(config)#show int e 1/1
100GigabitEthernet1/1 is down(interlaken crc error), line protocol is down
  STP Root Guard is disabled, STP BPDU Guard is disabled
  NP transmitted 0 packets, Received from TM 0 packets
```

The **show sysmon config** CLI command will display the configuration details for ILKN CRC monitoring. Action is none by default. If **sysmon np Interlaken-monitor crc-port-shutdown** is configured, action will be displayed as DISABLE-PORTS. Mode will be displayed as POLLING by default and if the feature is disabled, then it will displayed as DISABLED. Poll period will display the value as 30 seconds, which is the global default configuration for this feature.

```
device(config)#show sysmon config
------------------------+-------+-------------------------+----------+-----------+------------
+-----------------+---------------------
EVENT            |ACTION|SLOTS                    |MODE      |POLL PERIOD| THRESHOLD  |LOGBACK-OFF
                       |            |                                  |                |
(SEC)           | #(PER POLL |
                       |            |                                  |                |  in
#POLL)      |                       |
------------------------+--------+-------------------------+-------------+-------------------
+-------------------+---------------------
NP ILKN          |NONE    | BR-MLX-100Gx2   |POLLING  |     30              |     N/A             |  N/A
Monitoring
```

History

Release version	Command history
Extreme NetIron Software Release 5.8.00	These commands were introduced.

10Gx24-port interface module

For maximum performance, you will need to change the `system-init tm-credit-size` to `credit_1024b` for the 10Gx24-port interface module.

10Gx24-port interface module CLI commands

To change the system tm credit size to 1024b, enter the following commands.

The following CLI tasks are performed in the configuration level of the CLI.

> **NOTE**
> It is important to issue commands to `write memory` and `reload` the device after you enter the **system-init tm-credit-size credit_1024b** command.

1. Enter the configuration level of the CLI.

   ```
   device# config
   ```

2. Change the `system-init tm-credit-size` to `credit_1024b`.

   ```
   device(config)# system-init tm-credit-size credit_1024b
   ```

3. Exit the configuration level of the CLI.

   ```
   device(config)# exit
   ```

4. Issue command to `write memory` to the device.

   ```
   device# write memory
   ```

5. Issue command to `reload` the device.

   ```
   device# reload
   ```

The following example demonstrates the CLI commands necessary to change the `system-init tm-credit-size` to `credit_1024b` for the 10Gx24-port interface module.

```
device# config
device(config)# system-init tm-credit-size credit_1024b
device(config)# exit
device# write memory
device# reload
```

MLX 24-port 10Gbps (BR-MLX-10Gx24-DM) Interface Modules

The following figure shows the front panel of the BR-MLX-10Gx24-DM interface module.

The 24-port, 10 Gbps interface module (BR-MLX-10Gx24-DM) provides twenty four 10 Gbps ports that support SFP+ optics.

The BR-MLX-10Gx24-DM interface module supports 4.5 GB buffering per module.

BR-MLX-10Gx24-DM module is an oversubscribed module. The module can support up to 200Gbps when the system fabric mode is in Turbo mode (i.e. system has only Gen 2 and Gen 3 modules such as 8x10G, 100G or 24x10G modules). The module can support up to 12 10G wire-speed ports when the system fabric mode is in Normal mode (i.e. system also has any Gen 1 modules such as 1G or 4x10G modules).

The front panel includes the following features:

- Arrow-shaped LEDs in center horizontal strip for all ports. LEDs to the left support the top ports, LEDs to the right (pointing down) support the bottom ports.
- Twenty four 10G Ethernet ports

The following table describes the LEDs for the BR-MLX-10Gx24-DM interface modules.

TABLE 13 BR-MLX-10Gx24-DM module LEDs

Position	State	Meaning
Arrow-shaped LEDs in center horizontal strip between ports. Left LEDs support upper ports. Right LEDs support lower ports.	Solid green	A link has been established.
	Green blinking	The port is transmitting and receiving packets.
	Off	No link exists, and the port is not transmitting or receiving packets.

Power supply requirements for BR-MLX-10Gx24-DM modules

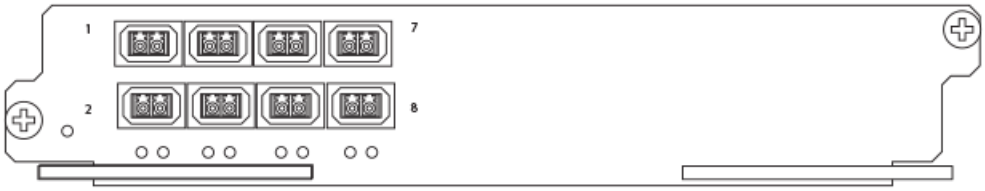
For power supply requirements for BR-MLX-10Gx24-DM interface modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

8x10GE-X interface modules

The 8x10GE-X interface modules provide 8 ports of 10 Gigabit Ethernet with support for up to 1M IPv4 routes in hardware.

> **NOTE**
> Gen-2 8x10GE-X modules require high speed switch fabric modules to operate. You can replace switch fabric modules with high-speed switch fabric modules while the system is powered on and running. For more information about high-speed switch fabric modules, refer to High-speed switch fabric modules on page 77.

FIGURE 8 8x10GE-X module faceplate



8x10GE-X modules support SFP+ optics only; they do not support SFP or XFP optics. For a list of supported SFP+ optics, refer to the latest version of the *Extreme Optics Family Data Sheet*.

8x10GE-X interface module LEDs

The following table describes the module and port LED status for the 8x10GE-X interface module.

TABLE 14 8x10GE-X module LEDs

LED	Location	State	Meaning
Power	Lower left corner of module	Green	Module is receiving power
		Off	Module is not receiving power
Link/Act	Below the ports. Top port LED on left, bottom port LED on right.	Green blinking	Port enabled and link is passing traffic. LED is solid green when link is idle.
		Off	Port is disabled.

Power supply requirements for 8x10GE-X modules

For power supply requirements for the 8x10GE-X modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

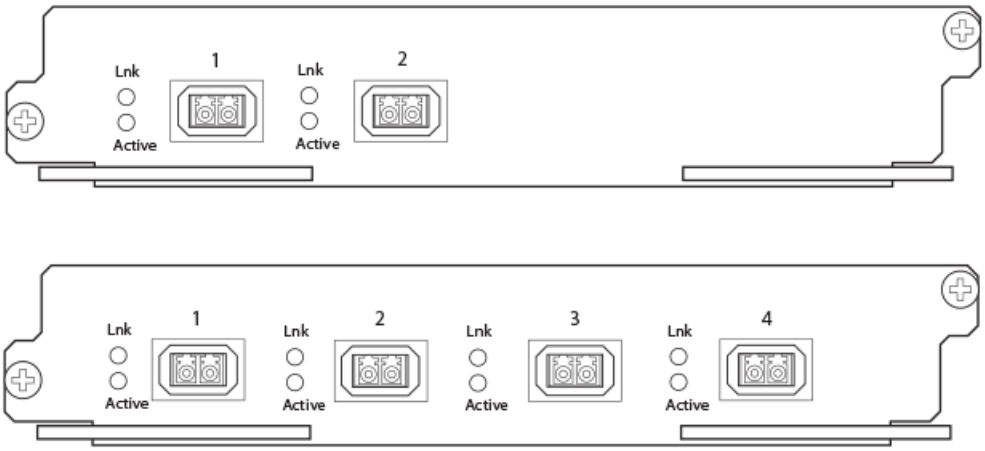
Gen-1 10Gx2 and 10Gx4 Ethernet interface modules

Gen-1 2-port and 4-port 10 Gbps Ethernet interface modules are available in the following formats:

- NI-MLX-10Gx2 - 2-port interface module for MLX devices
- NI-XMR-10Gx2 - 2-port interface module for XMR devices
- NI-MLX-10Gx4 - 4-port interface module for MLX devices
- NI-XMR-10Gx4 - 4-port interface module for XMR devices

NOTE
When you install Gen-1 2-port or 4-port 10 Gbps Ethernet interface modules, you must upgrade the software on all interface modules and management modules to the appropriate software release. For more information on the appropriate software release refer to the Hardware Installation Notes that shipped with the interface module.

FIGURE 9 Gen-1 2-port and 4-port 10 Gbps Ethernet module front panels



The front panel of the 2-port module includes two LEDs per port and two 10 Gpbs Ethernet XFP optics ports.

The front panel of the 4-port module includes two LEDs per port and four 10 Gpbs Ethernet XFP optics ports.

The table in the following section shows the meaning of each LED state.

10 Gbps Ethernet interface module LEDs

The following table describes the port LED status for the Gen-1 2-port and 4-port interface modules.

TABLE 15 Gen-1 2-port or 4-port 10 Gbps Ethernet module LEDs

LED	Location	State	Meaning
Link	Left of each Ethernet port	On	A link is established with the remote port.
		Off	A link is not established with the remote port.
Active	Left of each Ethernet port	On	The port is transmitting and receiving packets.
		Off	The port is not transmitting or receiving packets.

10 Gbps Ethernet ports

The Gen-1 2-port or 4-port Ethernet modules (BR-MLX-10Gx4-X) have either two or four physical ports that allow you to connect your router to other network routers at a speed of 10 Gbps.

You must insert XFP-compliant fiber-optic transceivers in each port you intend to use. XFP-compliant transceivers provide an optical or physical medium-dependent (PMD) interface for single- or multi-mode fiber that can be used with either the LAN physical layer (PHY) or WAN physical layer (WAN PHY).

For a list of XFP-compliant fiber-optic transceivers supported for Gen-1 2-port or 4-port modules, refer to the latest version of the *Extreme Optics Family Data Sheet*.

For more information about fiber-optic transceivers and associated cabling, refer to Installing a fiber-optic transceiver on page 197.

Power supply requirements for Gen-1 2-port or 4-port 10 Gbps Ethernet interface modules

For power supply requirements for Gen-1, 2-port or 4-port 10 Gbps Ethernet interface modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

BR-MLX-10GX4-X and BR-MLX-10Gx4-X-ML interface module LEDs

The following table describes the port LED status for the BR-MLX-10GX4-X and BR-MLX-10Gx4-X-ML interface module LEDs.

TABLE 16 BR-MLX-10GX4-X and BR-MLX-10Gx4-X-ML Ethernet module LEDs

LED	Location	State	Meaning
Link	Left of each Ethernet port	On	A link is established with the remote port.
		Off	A link is not established with the remote port.
Active	Left of each Ethernet port	On	The port is transmitting and receiving packets.
		Off	The port is not transmitting or receiving packets.

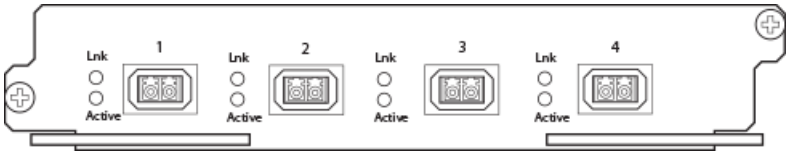
Gen-1.1 4-port 10 Gbps Ethernet interface modules

Gen-1.1 4-port 10 Gbps Ethernet interface modules are available in the following formats:

- BR-MLX-10Gx4-X-ML - 4-port interface module
- BR-MLX-10Gx4-X - 4-port interface module licensed for 1 million routes

NOTE
The 10Gx4-X10 GbE module requires a minimum software version of R05.1.00. Please upgrade all software on the system to a minimum of R05.1.00 before installing your 10Gx4-X module.

FIGURE 10 BR-MLX-10Gx4-X and BR-MLX-10Gx4-X-ML interface module front panel



The front panel of the BR-MLX-10GX4-X and BR-MLX-10Gx4-X-ML modules includes the following features:

- Two LEDs per port
- Four 10 Gbps Ethernet XFP optics ports

BR-MLX-10GX4-X and BR-MLX-10Gx4-X-ML interface module Ethernet ports

The BR-MLX-10GX4-X interface module has four physical ports that allow you to connect your router to other network routers at a speed of 10 Gbps. BR-MLX-10Gx4-X-ML supports up to 512K IPv4 routes in hardware. BR-MLX-10Gx4-X supports up to 1M IPv4 routes. BR-MLX-10Gx4-X-ML can be upgraded to an X version through a software license. Please contact Extreme Networks to purchase the license upgrade.

You must insert XFP-compliant fiber-optic transceivers in each port you intend to use. XFP-compliant transceivers provide an optical or physical medium-dependent (PMD) interface for single- or multi-mode fiber that can be used with either the LAN physical layer (PHY) or WAN physical layer (WAN PHY).

For an up to date list of the 10 Gbps XFP-compliant fiber-optic transceivers that are available from Extreme Networks, refer to the latest version of the *Extreme Optics Family Data Sheet*.

For more information about fiber-optic transceivers and associated cabling, refer to Installing a fiber-optic transceiver on page 197.

Power supply requirements for 10Gx4 interface modules

For power supply requirements for the 10Gx4 modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

8-port 10 Gbps M and D interface modules

For MLX Series routers, the 8-port, 10 Gbps interface modules (NI-MLX-10Gx8-M and NI-MLX-10Gx8-D) provide eight 10 Gbps ports that support SFP+ optics. These modules contain an internal flash memory of 16 MB for local storage of CPU images, and 32 MB for local storage of FPGA images. The NI-MLX-10Gx8-M interface module supports a buffer of 3 GB buffering per module. The NI-MLX-10Gx8-D module supports 1 GB buffering per module.

> **NOTE**
> When installing NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules, you must first upgrade the software on all interface modules and management modules to Multi-Service IronWare software R05.0.00 or later. For more information, refer to the Hardware Installation Notes that shipped with the modules.

> **NOTE**
> NI-MLX-10Gx8-D interface modules do not support MPLS.

> **NOTE**
> NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules require high-speed switch fabric modules to operate. You can replace switch fabric modules with high-speed switch fabric modules while the system is powered on and running. For more information about high-speed switch fabric modules, refer to High-speed switch fabric modules on page 77.

FIGURE 11 NI-MLX-10Gx8-M and NI-MLX-10Gx8-D module faceplate

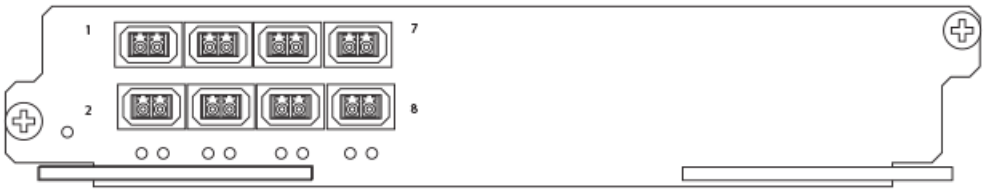
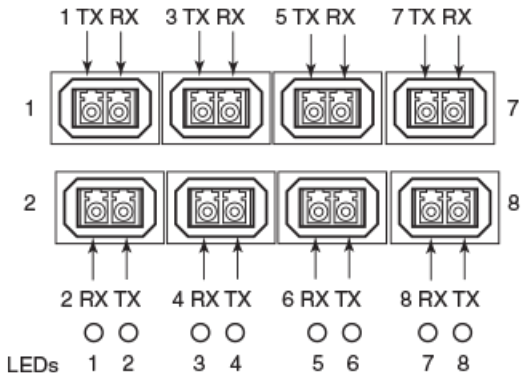


FIGURE 12 Port RX and TX, and LED designations for NI-MLX-10Gx8-M and NI-MLX-10Gx8-D modules



NI-MLX-10Gx8-M and NI-MLX-10Gx8-D modules support the SFP+ optics; they do not support SFP optics. For a list of supported SFP+ optics, refer to the latest version of the *Extreme Optics Family Data Sheet*.

NI-MLX-10Gx8-M and NI-MLX-10Gx8-D interface module LEDs

The following table describes the module and port LED status for the NI-MLX-10Gx8-M and NI-MLX-10Gx8-D interface module.

TABLE 17 NI-MLX-10Gx8-M and NI-MLX-10Gx8-D interface module LEDs

LED	Location	State	Meaning
Power	Lower left corner of module	Green	Module is receiving power
		Off	Module is not receiving power
Link/Activity	Underneath the ports. Top port LED on left, bottom port LED on right.	Green blinking	Port enabled and link is up.
		Off	Port is disabled.

Installation considerations

When you install NI-MLX-10Gx8-M or NI-MLX-10Gx8-D modules, you must upgrade the software on all interface modules and management modules to the appropriate software release. Refer to the Hardware Installation Notes that shipped with the interface module.

> **NOTE**
> NI-MLX-10Gx8-D modules do not support Multiprotocol Label Switching (MPLS).

If you try to configure MPLS on a device that has NI MLX 8x10G -D modules installed, you will see the following error message.

```
device(config)# router mpls
The command can't be used when system contains -d class modules.
```

If you install an NI-MLX-10Gx8-D module in a device that is running MPLS, the NI-MLX-10Gx8-D module boots in INTERACTIVE mode, and the following error message is displayed.

```
device#
Module is inserted into slot 7
SYSLOG: May 28 16:22:35:<13May 28 16:22:35 System: Module was inserted to slot 7
Module 7 is -d class, it can't work when router mpls is enabled.
Reset slot 7
SYSLOG: May 28 16:22:48 :<13>May 28 16:22:48 Module 7 is reset by mgmt (reason: boot to interactive mode)
```

Power supply requirements for NI-MLX-10Gx8-M and NI-MLX-10Gx8-D modules

For power supply requirements for NI-MLX-10Gx8-M and NI-MLX-10Gx8-D modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

24-port 1 Gbps Ethernet copper RJ-45 interface module

The 24-port 1 Gbps Ethernet copper interface module is available in the following formats:

- BR-MLX-1GCx24-X-ML
- BR-MLX-1GCx24-X

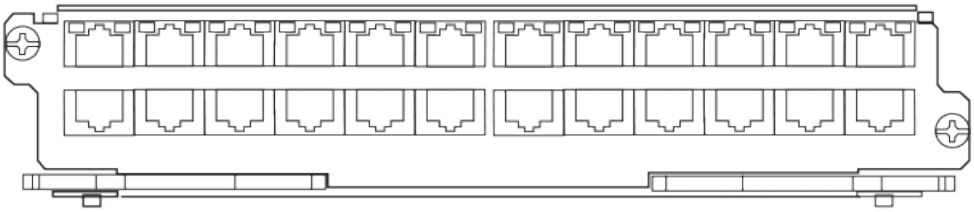
This module has 32 Mb of flash memory and contains 24 RJ-45 physical ports, through which you can connect your router to other network routers. BR-MLX-1GCx24-X-ML support s up to 512K IPv4 routes in hardware and BR-MLX-1GCx24-X version supports up to 1M IPv4 routes in hardware. BR-MLX-1GCx24-X-ML does not include a software license, but can be upgraded to an X version through a software license. Please contact Extreme Networks to purchase the license upgrade.

NOTE
When you install BR-MLX-1GCx24-X modules, you must upgrade the software on all interface modules and management modules to the appropriate software release. For more information on the appropriate software release refer to the Hardware Installation Notes that shipped with the modules.

NOTE
When you are replacing older modules with 24x1G modules, you must first delete the software configuration for the older module. If you do not delete the old configuration, a configuration mismatch will occur when you install the new module. This mismatch will be displayed in the results of the **show config** command.

NOTE
The SNMP Management Information Base (MIB) uses the Interface Index (ifIndex) to assign a unique value to each port on a module or slot. 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 installing 24-port copper or fiber interface modules, you must change the ifIndex allocation to 64 before you install the module, or the module will not operate properly.

FIGURE 13 BR-MLX-1GCx24-X copper interface module front panel



The front panel includes the following features:

- LEDs to the left support the top ports, LEDs to the right support the bottom ports
- 24 1 Gbps RJ-45 copper ports

The following table describes the port LED status for the BR-MLX-1GCx24-X copper module.

TABLE 18 BR-MLX-1GCx24-X copper module LEDs

Position	State	Meaning
LEDs located at top right and left edge of top row ports. Left LED for top port, right LED for bottom port)	Solid green	A link has been established.
	Green blinking	The port is transmitting and receiving packets.
	Off	No link exists and the port is not transmitting or receiving packets.

Power supply requirements for BR-MLX-1GCx24-X interface modules

For power supply requirements for BR-MLX-1GCx24-X interface modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

24-port 1 Gbps fiber interface module

The 24-port 1 Gbps fiber interface module is available in the following formats:

- BR-MLX-1GFx24-X
- BR-MLX-1GFx24-X-ML

The 24-port 1 Gbps fiber interface modules has 32 Mb of flash memory and provide 24 physical ports, through which you can connect your router to other network routers. BR-MLX-1GFx24-X-ML supports up to 512K IPv4 routes in hardware. BR-MLX-1GFx24-X supports up to 1M IPv4 routes in hardware. The ML version can be upgraded to a X version through a software license. Please contact Extreme Networks to purchase the license upgrade.

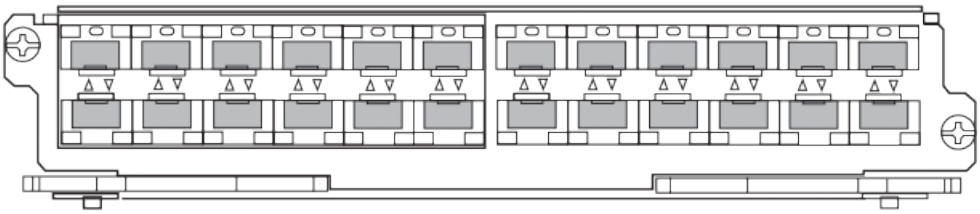
NOTE
24-port 1 Gbps fiber interface modules support 1 Gbps Copper SFP optics at 10 Mbps, 100Mbps and 1Gbps speeds.

NOTE
When you install BR-MLX-1GFx24-X and BR-MLX-1GFx24-X-ML modules, you must upgrade the software on all interface modules and management modules to the appropriate software release. For more information on the appropriate software release refer to the Hardware Installation Notes that shipped with the modules.

NOTE
When you are replacing older modules with 24x1G modules, you must first delete the software configuration for the older module. If you do not delete the old configuration, a configuration mismatch will occur when you install the new module. This mismatch will be displayed in the results of the **show config** command.

NOTE
The SNMP Management Information Base (MIB) uses the Interface Index (ifIndex) to assign a unique value to each port on a module or slot. 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 installing 24-port copper or fiber interface modules, you must change the ifIndex allocation to 64 before you install the module, or the module will not operate properly when installed.

FIGURE 14 BR-MLX-1GFx24-X and BR-MLX-1GFx24-X-ML fiber interface module front panel



The front panel includes the following features:

- Arrow-shaped LEDs in center horizontal strip for all ports. LEDs to the left support the top ports, LEDs to the right (pointing down) support the bottom ports.
- 24 1 Gbps fiber ports

The following table describes the port status for the BR-MLX-1GFx24-X and BR-MLX-1GFx24-X fiber module.

TABLE 19 BR-MLX-1GFx24-X and BR-MLX-1GFx24-X fiber module LEDs

Position	State	Meaning
Arrow-shaped LEDs in center horizontal strip between ports. Left LEDs support upper ports. Right LEDs support lower ports.	Solid green	A link has been established.
	Green blinking	The port is transmitting and receiving packets.
	Off	No link exists, and the port is not transmitting or receiving packets.

For a list of SFP optics supported for the BR-MLX-1GFx24-X and BR-MLX-1GFx24-X interface modules, refer to the latest version of the *Extreme Optics Family Data Sheet*.

Power supply requirements for BR-MLX-1GFx24-X and BR-MLX-1GFx24-X-ML interface modules

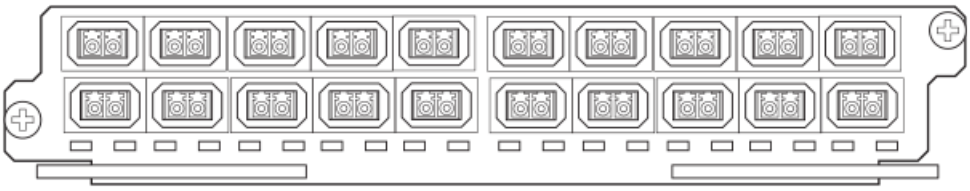
For power supply requirements for BR-MLX-1GFx24 and BR-MLX-1GFx24-X ML (24-port 1 Gbps) fiber interface modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

20-port 100/1000 Ethernet interface module

The front panel includes the following features:

- LEDs to the left support the top ports, LEDs to the right support the bottom ports
- 20 100/1000 Ethernet SFP ports

FIGURE 15 20-port 100/1000 Ethernet module front panel



The following table describes the port LED status of the 20-port 100/1000 Ethernet module.

TABLE 20 20-port 100/1000 Ethernet module LEDs

Position	State	Meaning
Below each Ethernet port.	On or blinking	The port is transmitting and receiving packets.
(Left-side LED supports port in top row. Right-side LED supports port in bottom row.)	Off for an extended period	The port is not transmitting or receiving packets.

100/1000 Ethernet ports

The 100/1000 Ethernet interface module contains 20 physical ports, through which you can connect your router to other network routers at a speed of 100 Mbps or 1 Gbps.

You must insert an SFP-compliant fiber-optic transceiver (provided by Extreme) into a physical port. SFP-compliant fiber-optic transceivers provide a physical medium-dependent (PMD) fiber interface that can be used with either the LAN physical layer (PHY) or WAN physical layer (WAN PHY).

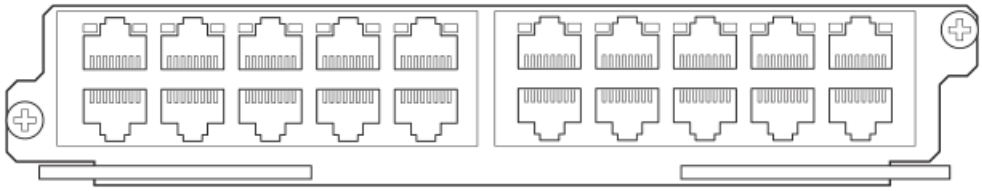
For a list of SFP optics supported by Extreme Networks, refer to the latest version of the *Extreme Optics Family Data Sheet*.

20-port 10/100/1000 Ethernet interface module

The front panel includes the following features:

- LEDs
- Twenty 10/100/1000 copper Ethernet ports.

FIGURE 16 20-port 10/100/1000 copper Ethernet interface module front panel



The following table describes the LED status for the 20-port 10/100/1000 copper Ethernet interface module.

TABLE 21 20-port 10/100/1000 Ethernet module LEDs

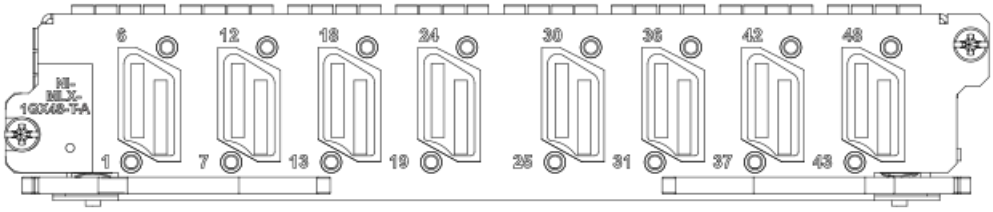
LED	Position	State	Meaning
Link or Active	Above the ports. The top port LED is on the left side, the bottom port LED is on the right side.	On (solid)	A link is established with the remote port (with no traffic).
		Blinking	The port is transmitting and receiving packets.
		Off	A link is not established with the remote port and no traffic is being passed.

NI-MLX-1Gx48-T-A interface module

The front panel includes the following features:

- A power LED located below the part number
- Eight mini-RJ21 connectors, each supporting six 10/100/1000 Mbps Ethernet ports

FIGURE 17 NI-MLX-1Gx48-T-A module front panel



The eight mini-RJ21 connectors support six 1 Gbps Ethernet ports each. You can connect a patch panel with a mini-RJ21 connector to a mini-RJ21 connector on the interface module. The patch panel provides RJ-45 connectors. You can also use a cable with a mini-RJ21 connector on one end that connects to the mini-RJ21 connector on the interface module. The other end of the cable splits into six cables with RJ-45 connectors on each cable.

> **NOTE**
> Starting with the Extreme NetIron software 5.6.00a code release, XMR-32 and MLX-32 systems will support a maximum of 25 NI-MLX-1GX48-T-A modules. If more than 25 NI-MLX-1GX48-T-A modules are currently installed in these systems and the code is upgraded to any Extreme NetIron patch or software release later than Extreme NetIron software R5.6.00 from a pre-5.6.00 Extreme NetIron release, the system will no longer recognize the remaining NI-MLX-1GX48-T-A modules. It is recommended that these excess modules be removed from the system and all references to these slots be removed from the startup configuration prior to upgrading to any Extreme NetIron R5.6.00 patch release.

The NI-MLX-1Gx48-T-A module ships with two cable cinches. Each cable cinch consists of a plastic part and a velcro strap. For instructions on using the cable cinches, refer to Using Extreme Structured Cabling Components on page 183.

Cables and patch panels that support this module are available through any Tyco International distribution partner. Information about these products is available at the following URL.

www.extremenetworks.com

> **NOTE**
> Before you install NI-MLX-1Gx48-T-A modules, you must first upgrade the software on all interface modules and management modules to the appropriate software release. For more information refer to the Hardware Installation Notes that shipped with the modules.

Power supply requirements for NI-MLX-1Gx48-T-A modules

For power supply requirements for NI-MLX-1Gx48-T-A interface modules, refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.

> **NOTE**
> When one or more NI-MLX-1GX48-T-A modules are installed in an MLX16-slot router, you must replace the NI-X-16-FAN-EXH modules with NIBI-16-FAN-EXH-A high-speed fan modules. For more information about high-speed fan modules, refer to NIBI-16-FAN-EXH-A high-speed fan assemblies on page 86. If the 16-slot router is not upgraded to support NIBI-16-FAN-EXH-A modules before NI-MLX-1GX48-T-A modules are installed, the following Syslog message is displayed.
> `SYSLOG: Mar 26 14:19:53:<12>R1, 48X1G modules in slots 10,11,13,16 shouldn't be running without high speed fans`

> **NOTE**
> The NIBI-16-FAN-EXH-A fan module does not ship with some MLX-16 routers. Contact Extreme Networks to purchase this module.

To display information about NIBI-16-FAN-EXH-A modules installed in a 16-slot router, enter the **show chassis** command.

```
device# show chassis
***  MLX Series-16 chassis ***
Power 1 (H1250CFN - AC 1200W): Installed (OK)
Power 2: Installed (Failed or Disconnected)
Power 3: not present
Power 4: Installed (Failed or Disconnected)
Power 5: (H1250CFN - AC 1200W): Installed (OK)
Power 6: (30351200 - AC 1200W): Installed (OK)
Power 7: Installed (Failed or Disconnected)
Power 8: (30351200 - AC 1200W): Installed (OK)
Total power budget for chassis = 4800 W
Total power used by system core = 762 W
Total power used by LPs = 1040 W
Total power available = 2998 W
Slot Power-On Priority and Power Usage:
Slot10 pri=1 module type=NI-MLX-1Gx48-T-A 48-port 10/100/1000Base-T MRJ21 Module power usage=260W
Slot11 pri=1 module type=NI-MLX-1Gx48-T-A 48-port 10/100/1000Base-T MRJ21 Module power usage=260W
Slot13 pri=1 module type=NI-MLX-1Gx48-T-A 48-port 10/100/1000Base-T MRJ21 Module power usage=260W
Slot16 pri=1 module type=NI-MLX-1Gx48-T-A 48-port 10/100/1000Base-T MRJ21 Module power usage=260W
--- FANS ----
Bottom fan tray (fan 1): Status = OK, Speed = LOW (50%)
Bottom fan tray (fan 2): Status = OK, Speed = LOW (50%)
Bottom fan tray (fan 3): Status = OK, Speed = LOW (50%)
Bottom fan tray (fan 4): Status = OK, Speed = LOW (50%)
Bottom fan tray (fan 5): Status = OK, Speed = LOW (50%)
Bottom fan tray (fan 6): Status = OK, Speed = LOW (50%)
Rev A Back Fan A (revision 0x09): Status = OK, Speed = LOW (50%)
Rev A Back Fan B (revision 0x0c): Status = OK, Speed = LOW (50%)
```

The output displays firmware Revision A (Rev A) for NIBI-16-FAN-EXH-A modules. Rev A indicates that the router contains the required rear fan modules to support the NI-MLX-1Gx48-T-A modules. The RPM value thresholds (LOW/MED/MED-HI/HI) are also displayed for rear fan modules.

If the router does not contain NIBI-16-FAN-EXH-A modules, the **show chassis** command will not display Rev A for rear fan modules.

BR-MLX-40Gx4-M 4-port 40GbE module

The front panel includes the following features:

- Name of the module.
- Number of ports and the type of ports.
- LED indicator for a port.
- LED indicator for module power.

FIGURE 18 BR-MLX-40Gx4-M module front panel

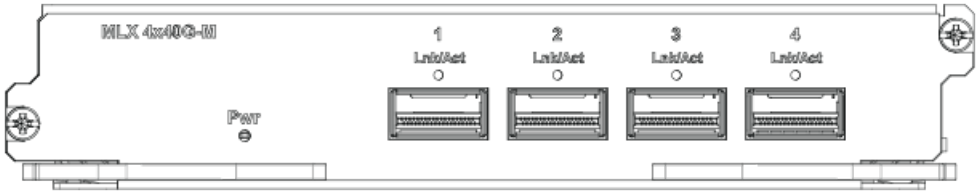
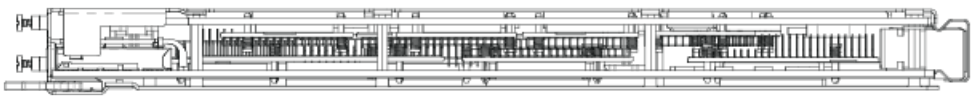


FIGURE 19 BR-MLX-40Gx4-M module front panel side view



The following table describes the port and module LED status for the BR-MLX-40Gx4-M module.

TABLE 22 BR-MLX-40Gx4-M module LEDs

LED	Position	State	Meaning
Link or Active	Above the ports	On (solid)	A link is established.
		Blinking	The port is transmitting and/or receiving.
		Off	A link is not established.
Power	Left side of front panel	On	Module is powered on.
		Off	Module is powered off.

The ExtremeRouting MLX Series 4-port 40 GbE (M) module includes Layer 2, IPv4/IPv6, MPLS and OpenFlow features, supports 512K IPv4 routes in the Forwarding Information Base (FIB), and requires high speed switch fabric modules and QSFP+ optics.

Module configuration: **System** > **Module** > **Add Module**

The GUI will add a new module from the selection menu using the following label:

```
BR-MLX-40GX4-M 4-port 40GbE Module
```

This new selection allows the configuration of the BR-MLX-40GX4-M 4-port 40GbE module.

Module display configuration: **System** > **Module**

The GUI will be modified to display a slot that has the configured 4x40GbE card.

Port Display configuration: **Port** > **Ethernet Port Attribute**

The GUI will be modified to display the appropriate optic type for 40GigE ports.

> NOTE
> Optics supported: 40G-QSFP-SR4 for 100M and 40G-QSFP-LR4 for 10KM.

> NOTE
> Safety requirements are the same as MLX 24x10G.

Auto-tuning links

Links brought down by CRC bursts and slow rate CRC receive auto-tuning before fabric link monitoring shuts down those links.

Auto-tuning links for burst CRC

Auto-tuning software will attempt to tune a link that is brought down by hardware due to a CRC burst, and when a slow rate CRC is encountered, before fabric link monitoring shuts down that link. This enhancement will use existing fabric link monitoring syslog, SFM log and SNMP trap messages for links shutdown or links powered down.

There are two instances when auto-tuning for a link is triggered:

- Slow rate CRCs are encountered.
- Burst CRCs are encountered.

> NOTE
> The feature for auto-tuning links for burst CRC was introduced in release 5.7.

Software sends a syslog/trap when auto-tuning is started and completed. This feature will utilize existing slow rate CRC auto tuning syslog and SFM logs.

In the case where slow rate CRCs are encountered, triggering fabric link monitoring, the CRC error counter of each link is polled for every monitoring period as follows:

- If the total CRC errors in monitoring period pass, slow rate CRC monitoring will start auto-tuning that particular link, instead of shutting down the link.
- If the tuning algorithm returns an error, or if the software attempts to start auto-tuning links that are already-tuned, software performs one of the following actions:
  - Link is powered down, sending a syslog and trap.
  - Link is not powered down, sending a syslog and trap (depending on the `sysmon` link configuration).

In slow rate CRC monitoring, link monitoring polls the CRC error counter of each link for every monitoring period. If the total CRC errors in monitoring period pass, link monitoring will start auto-tuning that particular link instead of shutting down the link.

Auto-tuning CLI commands

This topic covers the steps for executing the `sysmon fe auto-tune` and `sysmon tm auto-tune` for enabling or disabling auto-tuning on FE and TM for burst CRC.

Log into your system.

The following CLI steps will enable or disable auto-tuning on FE and TM for burst CRC.

1. Execute the CLI command `[no] sysmon fe auto-tune`.

   ```
   device(config)#sysmon fe auto-tune
   Event type already enabled.
   ```

   Enables or disables auto-tuning on FE for burst CRC.

   NOTE
   Default: Enabled.

2. Execute the CLI command `[no] sysmon tm auto-tune`.

   ```
   device(config)#sysmon tm auto-tune
   Event type already enabled.
   ```

   Enables or disables auto-tuning on TM for burst CRC.

   NOTE
   Default: Enabled.

The following example demonstrates the CLI command necessary to execute the `sysmon fe auto-tune` command for enabling high rate auto-tuning on FE for burst CRC.

```
devicedevice# sysmon fe auto-tune
```

The following example demonstrates the CLI command necessary to execute the `no sysmon fe auto-tune` command for disabling high rate auto-tuning on FE for burst CRC.

```
device# no sysmon fe auto-tune
```

The following example demonstrates the CLI command necessary to execute the `sysmon tm auto-tune` command for enabling high rate auto-tuning on TM for burst CRC.

```
device# sysmon tm auto-tune
```

The following example demonstrates the CLI command necessary to execute the `no sysmon tm auto-tune` command for disabling high rate auto-tuning on TM for burst CRC.

```
device# no sysmon tm auto-tune
```

Fabric link monitoring

Fabric monitoring will normally shutdown the link which was put down by hardware during burst CRCs. With auto tuning enabled, the link gets tuned for the first time when the link goes down, and if the same link goes down even after tuning, it gets powered down by fabric link monitoring.

Fabric link monitoring is running on MP only, and relies on the built-in hardware feature of the fabric element (FE) chipset sitting on the switch fabric. This hardware feature tracks the leaky bucket value. Initially, the leaky bucket value is set to the value of 63. For each cell with CRC, the FE will decrement the leaky bucket by the value of 1.

When the leaky bucket value is below the DOWN threshold, the FE marks the link as DOWN. For every 256 good cells received, the FE increment the leaky bucket value by 1 until it reaches the maximum value of 63. When the leaky bucket value passes the UP threshold, the FE marks the link as UP. The DOWN and UP thresholds are as follows:

- **DOWN threshold = 16**

  Leaky bucket < 16 change from UP to DOWN status.
- **UP threshold = 32**

  Leaky bucket > 32 change from DOWN to UP status.

  NOTE
  In certain scenarios, the link can be alternating UP to DOWN and DOWN to UP. When this happens, there is traffic loss in the system. To avoid this scenario, software fabric link monitoring will monitor the link status every second. The link is tuned once after the link is DOWN >= 10 times after a 20 second monitoring period. After tuning the link, if the link is DOWN again due to CRCs, then the link is powered down. However, the link is not powered DOWN with auto-tuning enabled; instead, the link gets tuned for the first occurrence of DOWN.

Forward Error Correction mode

Using Forward Error Correction (FEC) mode enabled modules on an MLX Series chassis will reduce packet drops due to CRC errors. FEC will automatically be enabled on supported line cards and fabric links in an ExtremeRouting MLX series chassis.

FEC mode is applicable for the MLX Series platforms. It will be operational on the 16Ke chassis and 32Ke chassis for the following cards:

- 2x100G
- 24x10G
- 4x40G
- hSFMs (FE600 based SFMs)

FEC mode is applied on a per link basis. Both sides of the link (TM side and FE side) must be in the same mode. In an MLX Series chassis, the following applies:

- All fabric facing links on the 4x40G, 2x100G and 24x10G TMs will have FEC enabled

- hSFM links connected to 4x40G, 2x100 and 24x10 will have FEC enabled

Forward Error Correction on Backplane Serdes Links

The operating margin of the longer backplane traces in the MLX Series 16Ke and 32e chassis may be reduced due to signal attenuation. In the normal coding scheme (8b/10b), CRC errors are detected and the corrupt packets are dropped.

The fabric is enabled in FEC mode by default on serdes links. Single-burst errors can be corrected on the fly, so packet drops are avoided.

Forward Error Correction (FEC) on Serdes-Mode Command

The fabric is in FEC mode by default. Therefore the **[no] serdes-mode** command will only have the **force-normal option**.

The **[no] serdes-mode** command is for MLX Series device installations with FEC on backplane serdes links only.

1. Enter the **[no] serdes-mode** command.

```
device# config
device(config)# system-init fabric-serdes-mode force-normal
```

```
device# config
device(config)# no system-init fabric-serdes-mode force-normal
```

2. Enter the **write memory** command.

```
device# write memory
```

3. Enter the **reload** command.

```
device# reload
```

Line Module Shutdown

Line Module Shutdown is an RAS feature that improves reliability of the XMR/MLX chassis. The LP card is shutdown when both MPs are down or MP's are disconnected from the chassis. L2 and L3 traffic is stopped, and the router stops forwarding all traffic.

Hardware flooding and dropping control traffic, required for processing by the router, is thereby avoided though the RAS feature of Line Module Shutdown.

Switch fabric modules

Switch fabric modules and high speed switch fabric modules that are available for MLX Series routers contain two LEDs, and can be configured with 4-slot routers, 8-slot routers, 16-slot routers, and 32-slot routers.

The following table shows the switch fabric modules that are available for MLX Series routers. For a detailed compatibility matrix of which fabric modules can be used with which router configurations, refer to the *Release Notes* for your software release.

TABLE 23 Switch fabric modules available for MLX Series routers

Part number	Description
NI-X-SF1	Switch fabric module for 4-slot routers
NI-X-SF3	Switch fabric module for 8- and 16-slot routers
NI-X-32-SF	Switch fabric module for 32-slot routers

The following table shows the high speed switch fabric modules that are available for MLX Series routers. For a detailed compatibility matrix of which fabric modules can be used with which router configurations, refer to the *Release Notes* for your software release.

TABLE 24 High speed switch fabric modules available for MLX Series routers

Part number	Description
NI-X-4-HSF	High speed switch fabric module for 4-slot routers
NI-X-16-8-HSF	High speed switch fabric module for 8- and 16-slot routers
NI-X-32-HSF	High speed switch fabric module for 32-slot routers

Switch fabric modules switch packets from one interface module to another. MLX Series routers can be configured with multiple switch fabric modules, and described as follows:

- 4-slot router: Accommodates three switch fabric modules (two required and one redundant) for a fully-loaded system. Ships with two switch fabric modules. You must purchase an additional switch fabric module to equip your router for redundancy.
- 8-slot router: Accommodates three switch fabric modules (two required and one redundant) for a fully-loaded system. Ships with two switch fabric modules. You must purchase an additional switch fabric module to equip your router for redundancy.
- 16-slot router: Accommodates four switch fabric modules (three required and one redundant) for a fully-loaded system. Ships with three switch fabric modules. You must purchase an additional switch fabric module to equip your router for redundancy.
- 32-slot router: Accommodates eight switch fabric modules. MLX Series routers ship with seven fabric modules. You must purchase an additional switch fabric module to equip your MLX Series router for redundancy.

  NOTE
  MLX Series router switch fabric modules are dedicated, which means that they function properly in these routers only. If you attempt to install a MLX Series router switch fabric module in another Extreme device or a switch fabric module intended for another Extreme device in a MLX Series router, the router and switch fabric module will not function properly.

The front panel contains two LEDs.

FIGURE 20 Switch fabric module front panel

TABLE 25 Switch fabric module LEDs

Pwr	Above Active LED	On	The module is receiving power.
		Off	The module is not receiving power.
Active	Below Pwr LED	On(4-, 8-, and 16-slot routers only)	The switch fabric is on (active) and ready to switch user packets.
		Blinking (32-slot routers only)	The switch fabric is on (active) and being accessed by the Management Module CPU. This indicates normal operation.

TABLE 25 Switch fabric module LEDs (continued)

			NOTE On devices supporting software version R05.3.00 and earlier, when you insert an SFM or during powering on the device, the Active LED was off for a short duration, up to 15 seconds because the monitoring of the Fabric module is stopped for this duration. After this delay, the LED indicated the monitoring status. In version R05.4.00 and later, the Active LED reads the switch fabric continuously even during module insertion or powering on the device, and thus the Active LED blinks.
		Off for extended period	The switch fabric is not active and cannot switch user packets.

High-speed switch fabric modules

> **NOTE**
> Gen-1 switch fabric modules and Gen-2 high-speed fabric (HSF) modules are not compatible and will not operate together in the same device.

HSF modules are supported on MLX Series routers, and are interoperable with all existing interface modules.

HSF modules are hot-swappable, which means you can install or replace them while the system is powered up and running.

> **NOTE**
> Do not remove or power-off all switch fabric modules on an MLX Series chassis while the device is up and running. Removing all the switch fabric modules from the device and then re-inserting them can cause the device to become unstable, resulting in protocol flaps and thereby traffic impact. A system reload is required to recover.

HSF modules can operate in normal mode or turbo mode but will boot in turbo mode only if all active interface modules are Gen-2 and Gen-3modules.

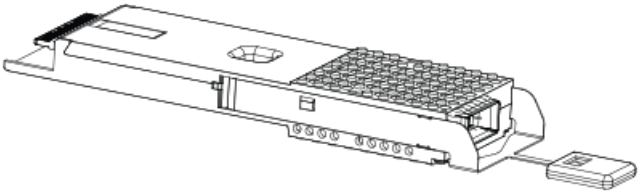
CFP2 to QSFP28 conversion module

This section provides general information about the Extreme CFP2 to QSFP28 conversion module, which installs into the 2x100GbE CFP2 optics based high density module of the MLX Series router.

> **NOTE**
> To install the conversion module, refer to instructions in section, Removing and Replacing a CFP2 to QSFP28 Conversion Module.

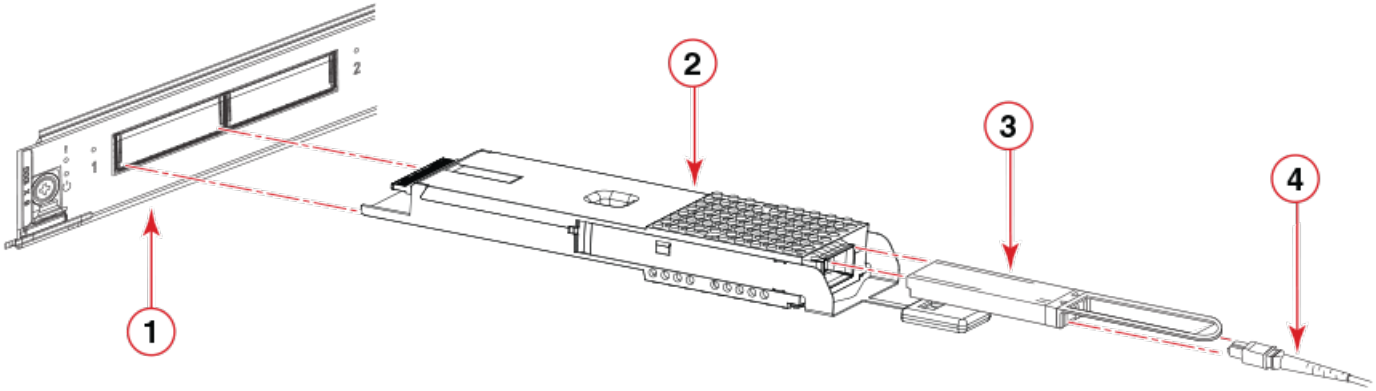
The CFP2 to QSFP28 conversion module in the following illustration inserts into 100 GbE CFP2 port cages (ports) on the 2x100GbE CFP2 optics based high density module to allow connection to 100 GbE QSFP28 ports.

FIGURE 21 CFP2 to QSFP28 conversion module



A QSFP28 transceiver plugs into the conversion module, and a QSFP cable connects to the transceiver, as shown in the following illustration.

FIGURE 22 Conversion module with QSFP28 transceiver and cable



1. 100 GbE CFP2 port
2. CFP2 to QSFP28 conversion module
3. 100 GbE QSFP28 transceiver
4. QSFP cable

100 GbE QSFP28 SR4 optics support Forward error correction (FEC). FEC enhanced data reliability by inserting redundant data, called error correcting code, into data being transmitted or stored. You can enable or disable FEC using the **fec** command in interface configuration mode.

The following example configures FEC on Ethernet interface 1/1:

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# fec
device(config-if-e10000-1/1)# end
```

> **NOTE**
> 100 GbE QSFP28 transceivers do not support breakout mode.

Use the following QSFP28 transceiver and optical cable for the conversion module:

- QSFP28 LR4, 2Km and 10Km transceiver
- QSFP28 SR4 transceiver
- 40GbE QSFP to QSFP cable, 10m AOC

QSFP28 form factor media must be installed in the conversion module.

The conversion module has a bicolor (green and amber) LED which functions as follows:

TABLE 26 LED descriptions

Color	Status	Recommended action
Amber	Conversion module and QSFP28 transceiver installed in 100 GbE port.	Connect cable to transceiver from 100 GbE port to complete connection.
Green	Cable from is connected from QSFP28 transceiver to the remote end and the link is active.	No action

Power supplies

Extreme Networks supports the following power supply types:

- 1200W AC or DC power supply
- 1800W AC or DC power supply
- 2100W AC or DC power supply
- 2400W AC or DC power supply
- 3000W AC or DC power supply

The following table lists the power supplies that are available for MLX Series routers.

TABLE 27 Power supplies

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

MLX Series routers support the following power supply options:

- 4-slot router: Can accommodate four 1200W or 1800W power supplies. For power redundancy, you must purchase additional power supplies depending on how you populate your router. For determining the number of power supplies required for redundancy, refer to Chapter 7, "Hardware Specifications".
- 8-slot router: Can accommodate up to four 1200W or 1800W AC and DC power supplies. Because power is supplied over a common power bus, any power supply installed in addition to the minimum required provides backup for any supply that fails. For power redundancy, you must purchase additional power supplies depending on how you populate your router. For determining the number of power supplies required for redundancy, refer to the "Hardware Specifications" in this documentation.

- 16-slot router: Can accommodate eight 1200W or 1800W AC and DC power supplies. Because power is supplied over a common power bus, any power supply installed in addition to the minimum required provides backup for any power supply that fails. For power redundancy, you must purchase additional power supplies depending on how you populate your router. For determining the number of power supplies required for redundancy, refer to the "Hardware Specifications" in this documentation.

  NOTE
  1800W AC power supplies support low and high line operation. For line voltages between 90 - 180, the power supply operates at 1200W. For line voltages between 180 - 264, the power supply operates at 1800W.

- 32-slot router: Supports 2100W AC, 2400W AC and DC, and 3000W AC and DC models. Accommodates eight power supplies. Because power is supplied over a common power bus, any power supply installed in addition to the minimum required provides backup for any power supply that fails. For power redundancy, you must purchase additional power supplies depending on how you populate your router. For determining the number of power supplies required for redundancy, refer to the "Hardware Specifications" in this documentation.

Power supply interoperability

For MLX Series routers, power supplies for the 4-slot, 8-slot, and 16-slot devices are interchangeable. Power supplies for the MLX Series 32-slot devices cannot be used in MLX Series 4-slot, 8-slot, or 16-slot devices.

For power supply specifications, refer to Power specifications on page 271.

Power supplies are installed in slots along the bottom of 8-slot, 16-slot, and 32-slot routers. Power supplies are installed in slots in the rear of 4-slot routers.

Power supplies provide power to all router components, share the workload equally, and report status to the management module. If the management module detects that a power supply has failed or overheated, the management module redistributes the workload of the failed power supply to the remaining power supplies.

Power supplies generally have three LEDs on the faceplate that provide status for input power, output power, and notification of alarms. If the input power and output power LEDs are on (steady green), the power supply is providing power to the router components. For more information about power supply LEDs, refer to the AC and DC power supply sections in Observing the LEDs on page 172.

NOTE
After a power supply is removed from a router, the software determines if there is enough power to operate all of the interface modules. If there is not enough power, some interface modules will be powered off.

NOTE
If you want to perform a hitless upgrade, replace one power supply unit at a time, and make sure the device has at least +1 redundancy at all times.

CAUTION
Remove the power cord from a power supply before you install it in or remove it from the device. Otherwise, the power supply or the device could be damaged as a result. (The device can be running while a power supply is being installed or removed, but the power supply itself should not be connected to a power source.)

NOTE
In the 32-slot router, you cannot unlatch and remove a power supply without first releasing the cord retainer and removing the power cord.

Rack mounting brackets

All routers ship with pre-installed mounting brackets that allow you to front-mount the router in a standard 19-inch (EIA310-D) rack. For instructions about how to mount the router in a rack, refer to the installation chapter that is appropriate for your router model.

You can also mid-mount your 4-, 8- or 16-slot router in a rack using the brackets that ship with the router. You simply remove the brackets from the front of the router and mount them midway along the sides of the router. For more information, see the installation chapter appropriated for your router model.

MLX Series routers can also be mounted in a EIA rack or 4-post rack using optional rack mount kits available from Extreme Networks. For information about how to install your MLX Series router in a EIA rack or 4-post rack, refer to EIA rack or 4-Post Rack Mount Kit contents on page 121.

Cooling system for MLX Series routers

The cooling systems for MLX Series routers contain the following components:

- 4-slot router: Equipped with one fan assembly that contains two 4-speed fans and two fan controllers to support redundancy.
- 8-slot router: Equipped with one fan assembly containing four 4-speed fans and four fan controllers to support redundancy.
- 16-slot router: Equipped with two high-speed fan assemblies. Each fan assembly contains two 4-speed fans with four fan controllers to support redundancy. High-speed fans are identified in the **show chassis** command output in the following manner:

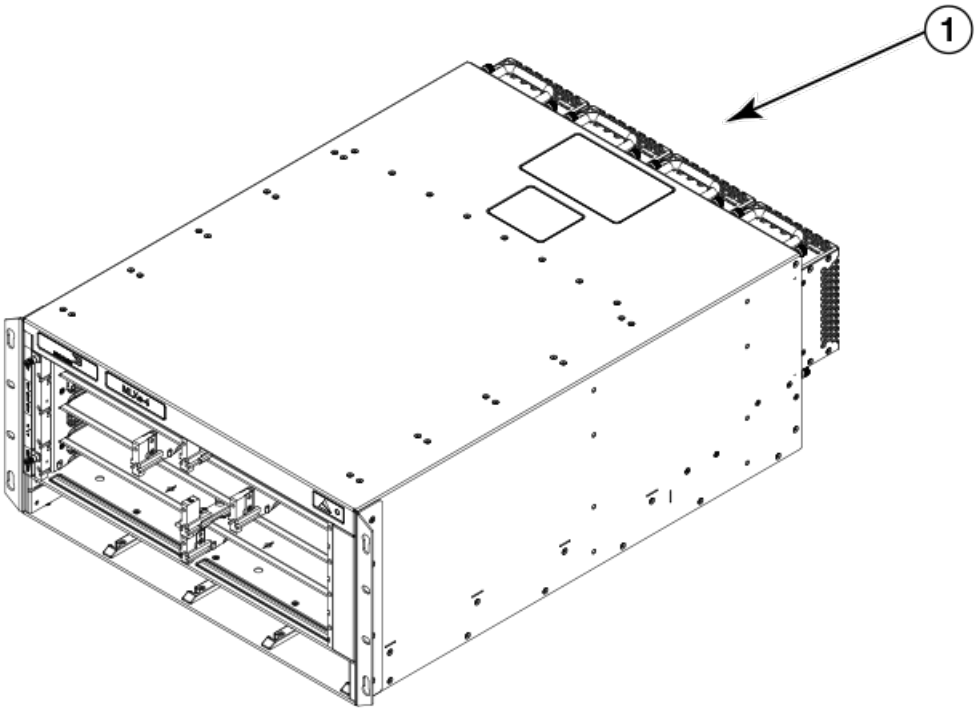
```
Rev A Back Fan A-1: Status = OK, Speed = LOW (50%)
Rev A Back Fan A-2: Status = OK, Speed = LOW (50%)
```

- 32-slot router: Equipped with ten fan assemblies. Each fan assembly contains a 4-speed fan. The fan trays support four settings, 50%, 60%, 75%, and 100%, as the normal fan speeds, which are set by the management module.

You can install an optional upward air deflector on the fans of 32-slot routers using a fan deflector kit from Extreme Networks.

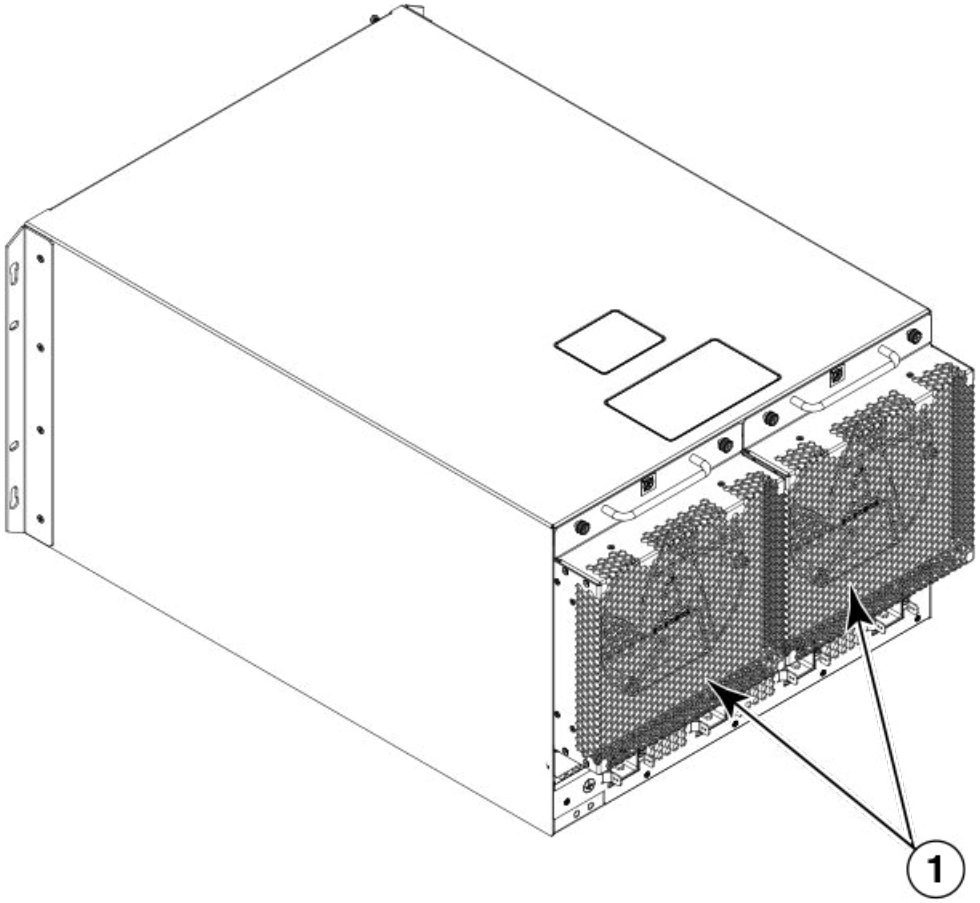
The following figures show the fan locations for 4- 8-, 16-, and 32-slot routers.

FIGURE 23 Fan locations for MLXe-4 routers



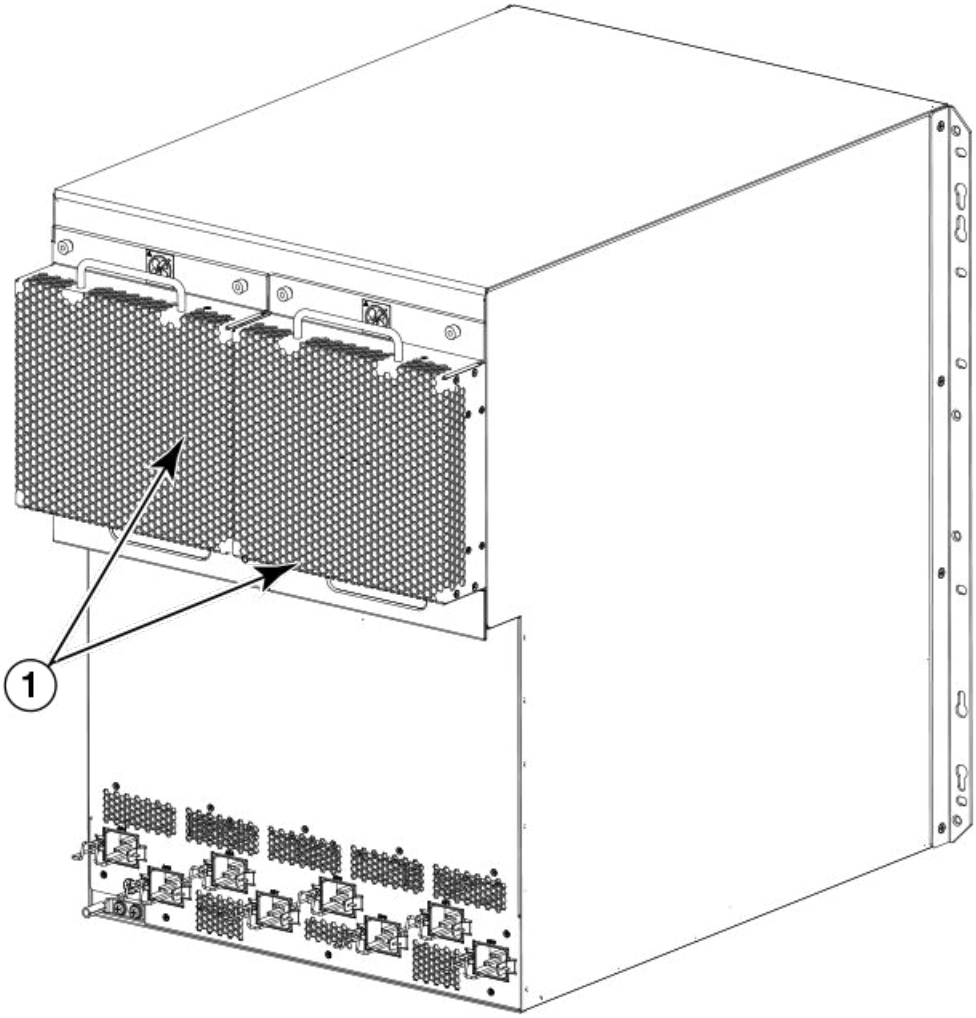
1. Fans in rear of chassis

FIGURE 24 Fan locations for MLXe-8-routers



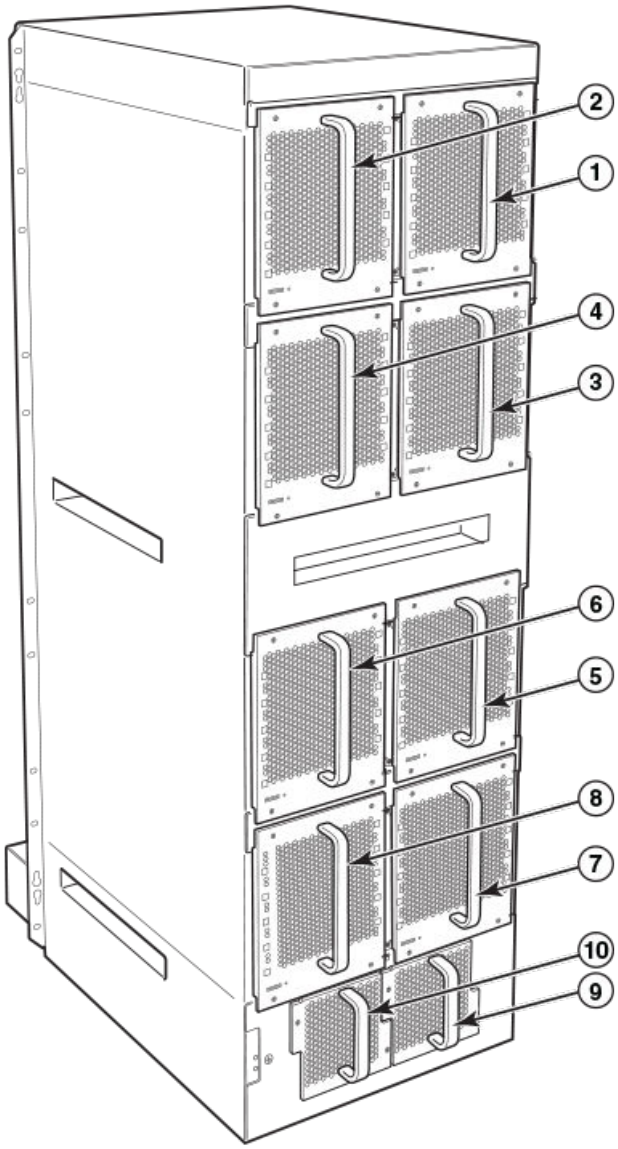
1. Fan modules

FIGURE 25 Rear fan location for MLXe-16 routers



1. Rear fan assemblies

FIGURE 26 Rear fan locations for MLXe-32-slot routers



1. Fan module 1
2. Fan module 2
3. Fan module 3
4. Fan module 4
5. Fan module 5
6. Fan module 6
7. Fan module 7
8. Fan module 8
9. Fan module 9
10. Fan module 10

At startup, the fans operate at high speed. After a period of time, the management module changes the fan speed to low.

By default, the router polls the temperature sensor on each module every 60 seconds for a temperature reading. Depending on the results, the router will:

- Leave the fan speed as is
- Increase the fan speed
- Decrease the fan speed

- Shut down a module to prevent damage

If the temperature of a module exceeds specified high temperature thresholds, the system generates a Syslog message and SNMP trap. The system can also shut down the module if the temperature exceeds the highest threshold.

You can change default low and high temperature thresholds for modules and fan speeds. Refer to Changing temperature thresholds for modules and fan speeds on page 211.

The fan control modules include a bi-color LED, which indicates the status of the fans. The following table describes the states of this LED.

TABLE 28 MLXe-32 router fan control LED

LED	Position	State	Meaning
Fan control LED	Rear of router on the fan assembly	Off	The fans are not receiving power.
		Green	The fans are working and responding to commands from the fan control module.
		Red	The fans are not working and not responding to commands the fan control module.

The router ships with fan assemblies fully installed. Fan assemblies are hot-swappable, which means you can remove and replace them without powering down the system.

NIBI-16-FAN-EXH-A high-speed fan assemblies

NIBI-16-FAN-EXH-A high-speed fan assemblies are required for MLXe-16 routers when you install NI-MLX-10Gx8-M, NI-MLX-10Gx8-D, or NI-MLX-1Gx48-T-A modules. MLXe-16 routers ship with high-speed fan assemblies factory installed. Refer to Replacing fan assemblies on page 255 for high-speed fan installation instructions.

Rack mount kit

MLX Series and XMR Series routers can be mounted in a standard 19-inch (EIA310-D) 2-post rack, using the pre-installed mounting brackets. For flush-mounting, simply use the mounting brackets as installed. For mid-mounting, move the pre-installed brackets from the front edges of the device to the holes provided in the sides of the device. For more information, refer to the appropriate installation chapter for your router model.

Supported software features

For a complete list of software features supported on the MLX Series routers, refer to the *Extreme NetIron Features and Standards Support Matrix, 6.2.00.*

Installing an ExtremeRouting MLX Series device

- Pre-Installation notice for the ExtremeRouting MLX chassis bundles....87
- Installation precautions....87
- Installing 2x100GbE CFP2 interface modules....91
- Installing BR-MLX-10Gx24-DM interface modules....92
- Installing an MLXe-4 router....93
- Installing an MLX-8 router....103
- Installing an MLXe-16 router....112
- Mounting the MLX-4, MLX-8 or MLX-16 router in a 4-post rack or EIA rack....121
- Installing an MLXe-32 router....134
- Attaching a management station....171
- Activating the power source....172
- Verifying proper operation....172

Pre-Installation notice for the ExtremeRouting MLX chassis bundles

The following software requirements must be met for any chassis bundle to operate properly.

- All MLXe-4 and MLXe-8 chassis bundle interface modules and management modules must be running the Extreme NetIron R05.0.00c or later.
- All MLXe-16 and MLXe-32 chassis bundle interface modules and management modules must be running the Extreme NetIron R05.0.00c or later.
- In certain module combinations, you will need to make sure the supported software is loaded.

  NOTE
  In certain module combinations, an MLX device may not have enough power supplies to support the configuration. Check the power specifications for the MLX chassis and the modules in the "Hardware Specifications" chapter of the installation guide to determine if an additional power supply is required. Additional power supplies can be ordered through Extreme Networks.

For additional information on upgrade procedures, refer to the *Extreme NetIron Software Upgrade Guide*.

Installation precautions

Read the following cautions and danger notices before installing MLX Series routers.

General precautions

DANGER
The procedures in this manual are for qualified service personnel.

DANGER
All fiber-optic interfaces use Class 1 lasers.

CAUTION
Do not install the device in an environment where the operating ambient temperature might exceed 40°C (104°F).

CAUTION
Make sure the airflow around the front, and back of the device is not restricted.

CAUTION
Do not drop any of the boards (cards) to be serviced or installed into the chassis as this may damage the board (card). For additional safety, cover hard surfaces with shock absorbent material in the work zone where the service or installation will be performed.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

CAUTION
Never leave tools inside the chassis.

Danger-general Shared

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Ein Gefahrenhinweis warnt vor Bedingungen oder Situationen die tödlich sein können oder Sie extrem gefährden können. Sicherheitsetiketten sind direkt auf den jeweiligen Produkten angebracht um vor diesen Bedingungen und Situationen zu warnen.

Un énoncé de danger indique des conditions ou des situations potentiellement mortelles ou extrêmement dangereuses. Des étiquettes de sécurité sont posées directement sur le produit et vous avertissent de ces conditions ou situations.

Una advertencia de peligro indica condiciones o situaciones que pueden resultar potencialmente letales o extremadamente peligrosas. También habrá etiquetas de seguridad pegadas directamente sobre los productos para advertir de estas condiciones o situaciones.

General dangers

DANGER
The procedures in this manual are for qualified service personnel.

GEFAHR	Die Vorgehensweisen in diesem Handbuch sind für qualifiziertes Servicepersonal bestimmt.
DANGER	Les procédures décrites dans ce manuel doivent être effectuées par un personnel de maintenance qualifié.
PELIGRO	Los procedimientos de este manual deben llevarlos a cabo técnicos cualificados.

DANGER
Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

GEFAHR	Die Finger dürfen nicht versehentlich in das Ventilatorblech gesteckt werden, wenn dieses vom Gehäuse abgenommen wird. Der Ventilator kann sich unter Umständen noch mit hoher Geschwindigkeit drehen.

DANGER	Faites attention de ne pas insérer vos doigts accidentellement dans le boîtier du ventilateur lorsque vous le retirez du châssis. Il est possible que le ventilateur tourne encore à grande vitesse.
PELIGRO	Procure no insertar los dedos accidentalmente en la bandeja del ventilador cuando esté desmontando el chasis. El ventilador podría estar girando a gran velocidad.

DANGER
This equipment is suitable for mounting on concrete or other noncombustible surfaces only.

GEFAHR	Dieses Gerät darf nur auf Beton oder auf andere, nicht brennbare Flächen installiert werden.
DANGER	Cet équipement est adapté à être monté sur du béton ou seulement sur d'autres surfaces non combustibles.
PELIGRO	Este equipo es apto para el montaje solamente en superficies de concreto ó en otro tipos de superficies no combustibles.

DANGER

GEFAHR	
DANGER	
PELIGRO	

Power precautions

CAUTION
Use a separate branch circuit for each power cord, which provides redundancy in case one of the circuits fails.

DANGER
Make sure to choose the appropriate circuit device depending on the number of AC power supplies installed in the chassis. The minimum current draw for the system is one AC power supply.

DANGER
Disconnect the power cord from all power sources to completely remove power from the device.

DANGER
Make sure that the power source circuits are properly grounded, then use the power cord supplied with the device to connect it to the power source.

DANGER
If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

CAUTION
Ensure that the device does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add the ampere (amp) ratings of all devices installed on the same circuit as the device. Compare this total with the rating limit for the circuit. The maximum ampere ratings are usually printed on the devices near the input power connectors.

CAUTION
All devices with DC power supplies are intended for installation in restricted access areas only. A restricted access area is a location where access can be gained only by trained service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

CAUTION
All devices with AC power sources are intended for installation in restricted access areas only. A restricted access area is a location where access can be gained only by trained service personnel through the use of a special tool, lock and key, or other means of security.

CAUTION
For the DC input circuit to the system of ExtremeRouting MLX-4, ExtremeRouting MLX-8, and ExtremeRouting MLX-16 routers (1800W supply), make sure there is a 60 amp circuit breaker, minimum -48VDC, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be copper wire, 6 AWG, marked VW-1, and rated minimum 90° C.

CAUTION
For the DC input circuit to the system of ExtremeRouting MLX-4, ExtremeRouting MLX-8, and ExtremeRouting MLX-16 routers (1200W supply), make sure there is a 40 amp circuit breaker, minimum -48VDC, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be copper wire, 6 AWG, marked VW-1, and rated minimum 90° C.

CAUTION
For the DC input circuit to the system of an ExtremeRouting MLX-32 (3000W supply) make sure there is a 80 amp circuit breaker, minimum -48Vdc, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be Listed copper wire, 2 AWG, marked VW-1, and rated minimum 90° C.

For the NEBS-compliant installation of MLX Series-4, MLX Series-8, and MLX Series-16 routers with a DC system:

CAUTION
For a DC system, use a grounding wire of at least 6 American Wire Gauge (AWG). The 6 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. For the Ground lug, use UL listed Panduit crimp connector, P/N LCD6-10A, and two 10-32, PPH, screws to secure crimp connector to chassis. Grounding position is located on the side of the chassis adjacent ground symbol.

For the NEBS-compliant installation of MLX Series-4, MLX Series-8, and MLX Series-16 routers with an AC system:

CAUTION
For an Extreme Networks AC system, use a ground wire of at least 6 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

For the NEBS-compliant installation of MLX Series-32, routers with a DC system:

CAUTION
For an ExtremeRouting MLX-32 DC system, use a grounding wire of at least 2 American Wire Gauge (AWG). The 2 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. Grounding position is located on the side of the chassis adjacent ground symbol.

For the NEBS-compliant installation of MLX Series-32, routers with an AC system:

CAUTION
For an ExtremeRouting MLX-32 AC system, use a ground wire of at least 2 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

Lifting precautions

DANGER
Make sure the rack housing the device is adequately secured to prevent it from becoming unstable or falling over.

DANGER
Mount the devices you install in a rack as low as possible. Place the heaviest device at the bottom and progressively place lighter devices above.

Installing 2x100GbE CFP2 interface modules

This section provides installation instructions for 2x100GbE CFP2 interface modules in an MLX Series device.

Installation considerations for 2x100GbE interface module

Before you install a 100xGbE 2-port interface, review the following installation considerations.

- The 2x100GbE module is a 1/2 height card, and occupies a 1/2 slot.
- If there is a module of another type installed, you must remove the existing module, and reconfigure the slot as **no module**.
- For maximum performance you must operate your 2x100GbE module with high speed switch fabric modules in turbo mode.

Installing 2x100GbE CFP2 interface modules

Before installing the 100GbE module in an MLX Series chassis, change **tm-credit-size** to 1024b (which readies the device to forward 100 Gbps traffic).

- 2x100GbE modules require a minimum software version of Extreme NetIron Software R05.7.00. Please upgrade all software on the system to a minimum version of R05.7.00 before you install your 100GbE module.
- 2x100GbE modules require high-speed switch fabric modules to operate.

NOTE
When installing modules, wear an ESD wrist strap.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

Log into your system and enter the following commands in the configuration level of the CLI, then write to memory and reload the device.

1. Upgrade the software on all management modules and interface modules to Extreme NetIron Software R05.7.00 or later. For specific upgrade instructions, refer to the *Extreme NetIron Software Upgrade Guide*.

2. Before you install your 2x100GbE CFP2 interface module into a working device, you must change the system **tm-credit-size** to 1024b (which readies the device to forward 100 Gbps traffic). Log into your system and enter the following commands in the configuration level of the CLI. Remember to write to memory and reload the device.

```
device# config
device(config)# system-init tm-credit-size credit_1024b
device(config)# exit
device# write memory
device# reload
```

NOTE
The **system-init tm-credit-size** command is only available in Extreme NetIron OS R05.7.00 or later, so it is important to upgrade all software to R05.7.00 or later before you install your 2x100GbE CFP2 module.

CAUTION
Do not use the port cover tabs to lift the module. They are not designed to support the weight of the module, which can fall and be damaged.

3. Insert the module into the slot until the connectors securely engage the backplane.

   In 4- and 8-slot devices, the modules are installed horizontally. In 16- and 32-slot devices the modules are installed vertically.

NOTE
The 2x100GbE CFP2 interface module is sensitive to dust and debris. Keep the optics covers in place until you are ready to connect the fiber cable. Clean all fiber cables properly before you connect them to the 2x100GbE CFP2 interface module.

Installing BR-MLX-10Gx24-DM interface modules

This section provides installation instructions for BR-MLX-10Gx24-DM interface modules.

Installation considerations

- BR-MLX-10Gx24-DM interface modules can be installed only in MLX Series devices running in MLX mode (NI-MLX-MR and BR-MLX-MR2-M or the equivalent 32 slot management modules).
- BR-MLX-10Gx24-DM interface modules are supported only on devices running Extreme NetIron Software R05.4.00 or later. For the latest upgrade instructions, refer to the *Extreme NetIron Software Upgrade Guide* on the Extreme Networks web site.
- Pull off the GBX connector cover before installing the module in the chassis.
- Use **show chassis** command to determine if you need additional power supplies.
- For installation in an MLXe-32 chassis, configure the chassis differently based on whether it has a Gen-1 module or not.
- The following conditions may prevent a BR-MLX-10Gx24-DM interface module from coming up properly:
  - BR-MLX-10Gx24-DM interface modules require the **snmp-server max-ifindex-per-module 40|64** configured. Otherwise, the cards will not come up.

NOTE
Not all features available in the Extreme NetIron Software R05.4.00 are supported on the BR-MLX-10Gx24-DM interface module. To verify if a particular feature is supported with the BR-MLX-10Gx24-DM interface module, refer to the latest version of the *Extreme NetIron Features and Standards Matrix.*

NOTE
For maximum performance, you must operate your BR-MLX-10Gx24-DM interface module with high speed switch fabric modules in turbo mode. For information on switch fabric modules, refer to Managing switch fabric modules on page 209.

Installation procedure

When installing modules, wear an ESD wrist strap with a plug for connection to the ESD connector on the router chassis or other suitable ground.

DANGER
For safety reasons, the ESD wrist strap should contain a 1 megohm series resistor.

1. Upgrade the software on all management modules and interface modules to Extreme NetIron Software R05.4.00 or later. For specific upgrade instructions, refer to the *Extreme NetIron Software Upgrade Guide*.
2. Configure the snmp maximum interface index per module to 64 using the **snmp-server max-ifindex-per-module 64** command

```
device (config)# snmp-server max-ifindex-per-module 64
```

3. For MLXe-32 installations only:
   a) If the chassis has a Gen-1 module, enter the following commands.

```
device# config
device(config)# system-init mlxe32-24x10g-enable max-tm-queue-4
device(config)# system-init fabric-data-mode force-normal
device# write memory
device# reload
```

   b) If the chassis has no Gen-1 module, enter the following commands.

```
device# config
device(config)# system-init mlxe32-24x10g-enable
device# write memory
device# reload
```

4. Install the BR-MLX-24x10G-DM module.
5. Verify that the module comes up,

NOTE
For known limitations, please refer to the Release Notes shipped with your module.

Installing an MLXe-4 router

This section describes how to install an MLXe-4 router.

Preparing the installation site

Before installing the router, plan the location and orientation relative to other devices and equipment. For cooling purposes, allow a minimum of six inches of space between the sides, front, and the back of the router and walls or other obstructions. If a router is installed in a perforated enclosure, the perforations must cover at least 60 percent of the surface.

NOTE
This equipment is suitable for installation in a Network Telecommunication facility and where NEC requirements apply. Additionally, it may be installed in either a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). It is not intended for Outside Plant (OSP) installations.

Ensure that the proper cabling is installed at the site.

For information on cabling, refer to Installing power supplies in an MLXe-4 router on page 99, Attaching a management station on page 171, and Connecting the router to a network device on page 197.

Unpacking an MLXe-4 router

The MLXe-4 router ships with the following items:

- Router chassis with switch fabric modules installed in slots marked SF, slot blanks installed in all empty module slots, and mounting brackets attached for front-mount.
- Insertion or extraction tool for use with RJ-45 and fiber-optic connectors.

NOTE
If any items are missing, contact the place of purchase.

Follow these steps to unpack your MLXe-4 router.

1. Remove the router from the shipping carton.
2. Save the shipping carton and packing materials in case you need to move or ship the router at a later time.

Installing an MLXe-4 router in an EIA rack

Your MLXe-4 router ships from the factory with mounting brackets attached. You can mount your router in the following ways:

- Front-mount in a standard two-post rack using the factory-installed brackets.
- Mid-mount in a standard two-post rack by moving the factory-installed brackets to the center of the device
- Mount the device in a four-post EIA rack using the EIA Rack Mount Kit. Refer to Installing MLXe-4 and MLXe-8 routers in a 4-post EIA rack on page 121.

NOTE
Because of the weight of a fully loaded MLXe-4 router, Extreme Networks recommends mounting it in a rack before installing the modules and AC power supplies.

You can install up to eight MLXe-4 routers in a standard 19-inch (EIA310-D) two-post rack using the factory-installed mounting brackets for either front- or mid-mounts.

Mounting your device in a standard 2-post rack

The factory-installed mounting brackets allow you to front-mount or mid-mount your device in the rack. For a mid-mount, you must remove the factory installed brackets from the front edge of the device and install them using the holes in the center-sides of the device. Refer to Figure 29.

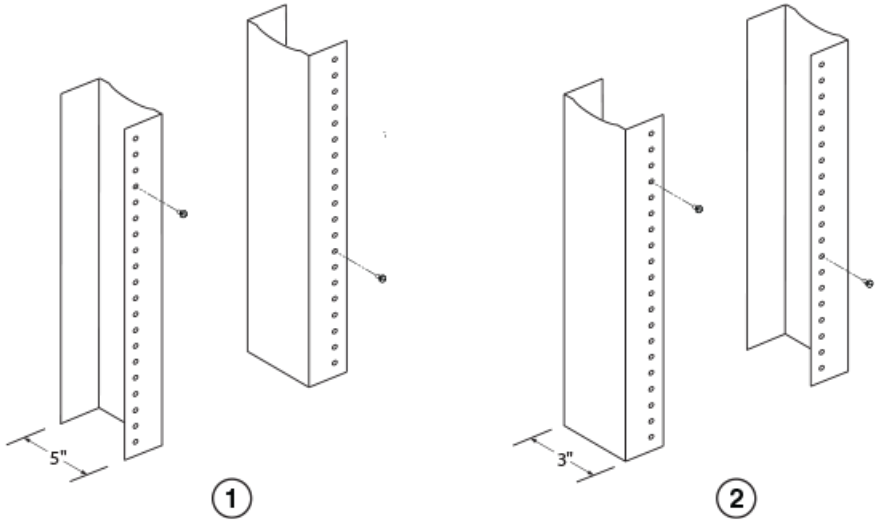
You will need to provide four standard #12-24 pan-head screws (per router) to secure routers in the rack. You will also need a #2 Phillips screwdriver. Complete the following steps.

NOTE
When connecting the device to the rack frame, use thread-forming screws and paint-piercing washers.

1. Determine the position of each router in the rack according to the weight of the router. For example, mount the router with the fewest modules near the top of the rack, a router with more modules near the middle of the rack, and fully populated routers near the bottom of the rack.
2. Using the keyhole slots in the router mounting brackets as a guide, align one screw per rack post, as shown in the following figure. On one side of the rack, the screw should align with the top hole in the mounting bracket. On the other side of the rack, the screw should align with the bottom hole of the mounting bracket. When tightening these screws, leave approximately 1/4 inch of clearance between the back of the screw head and the rack post.

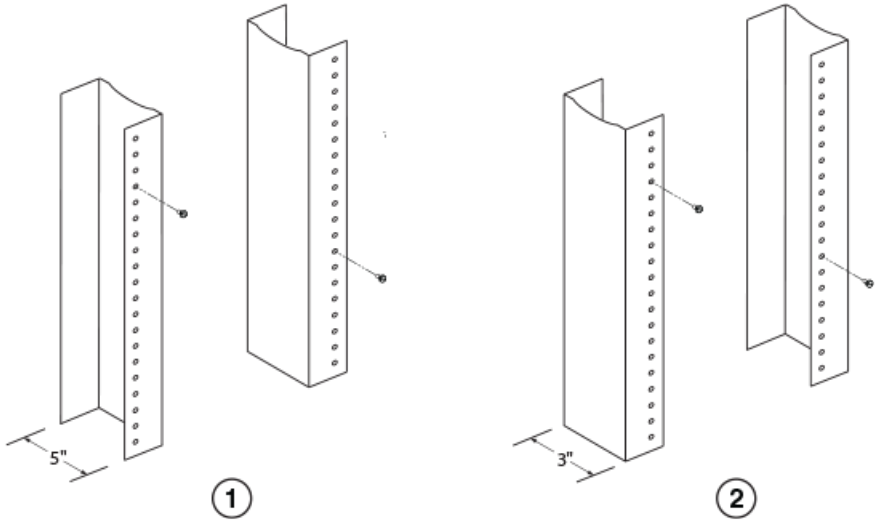
3. Mount the lowest router first. With one person on each side, lift the router and slip the widest part of each keyhole slot on the mounting bracket over the corresponding screw in the rack post, as shown in the following figure.

FIGURE 27 Positioning the mounting screws in rack posts



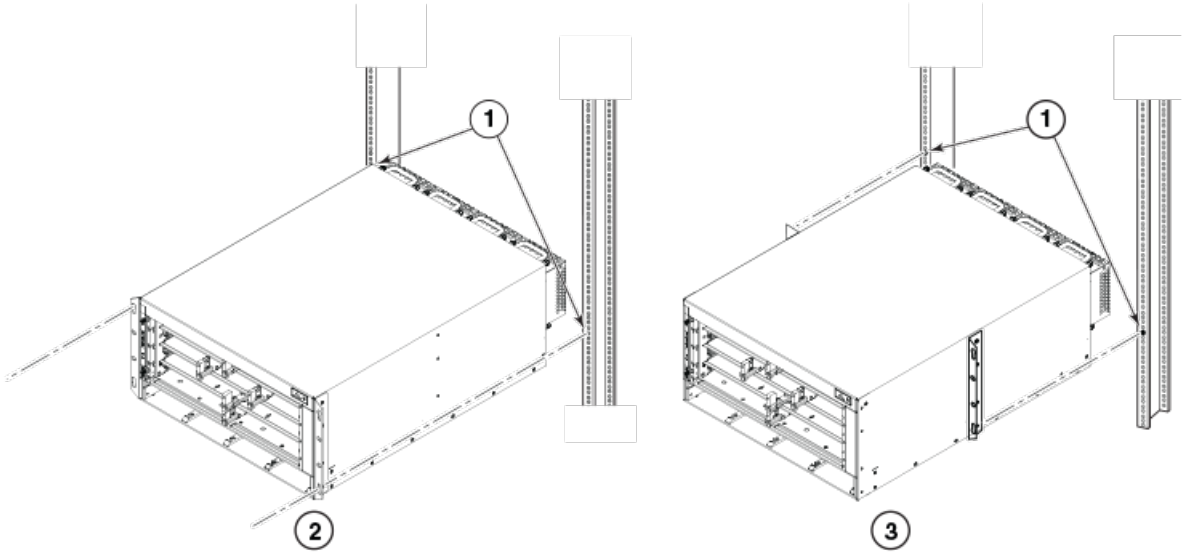
1. Unequal flange equipment rack
2. Network equipment rack

FIGURE 28 Positioning the mounting screws in rack posts



1. Unequal flange equipment rack
2. Network equipment rack

FIGURE 29 installing the router in a rack



1. Screws on mounting posts
2. Front-mount position
3. Mid-mount position

4. Slide the router down so that the mounting screw heads are in the narrowest part of the keyhole slots.
5. Tighten the screws to secure the router in place. For extra support, use additional screws.

   NOTE
   For better grounding of the router to the rack, attach the router using star washers. You should also use star washers with any single-hole grounding lugs to keep the lugs from rotating.

6. Repeat step 2 through step 5 to mount each router in the rack, moving from lowest to highest.

Installing MLXe-4 router modules

The sequence for installing multiple modules is important to ensure proper fit. The recommended sequence for the MLXe-4 router is to install right-to-left, beginning with the lowest row and moving up.

For instructions about installing 2x100GbE interface modules, refer to Installing 2x100GbE CFP2 interface modules on page 91.

For instructions about installing 2x100GbE interface modules, refer to Installing BR-MLX-10Gx24-DM interface modules on page 92.

NOTE
Installation procedures are identical for interface, management and switch fabric modules.

DANGER
The intra-building port or ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port or ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 5) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

NOTE
MLX Series modules are dedicated, which means that you must install them in MLX Series routers only. If you install a MLX Series module in a non- MLX Series router, or install a module intended for a non- MLX Series router in a MLX Series router, the router and module will not function properly. Although management modules are designed to be hot-swappable, you must upgrade the software on all interface modules and management modules to the appropriate software release before installing them. For more information on the appropriate software release, refer to the Hardware Installation Notes that shipped with the management module.

For information about how to disable and re-enable power to interface modules, refer to Disabling and re-enabling power to interface modules on page 224.

Modules must be installed in the correct slot number, as shown in the following list. First the slot number is shown, then the module into which it must be installed. An identifying label can be seen at the base of each slot.

NOTE
The MLXe-4 router ships with the required switch fabric modules installed.

1. Management modules
2. Active module - M1 (left).Redundant module - M2 (right).
3. Interface modules
4. - 4
5. Switch fabric modules
6. SF1 - SF3

If you are installing a redundant management module, refer to the chapter titled "Using a Redundant Management Module" in the MLX Series *and Extreme NetIron Family Configuration Guide* for information about how the redundant module works, optional software configurations, and how to manage redundancy.

You can install modules while the router is powered on and running.

Before installing a new interface module, you will need to remove the slot blank from the module slot. You should also have the following items available:

- A 1/4 inch #8 flat-blade screwdriver, or a #2 Phillips screwdriver
- A new interface module, which you can order from Extreme Networks.
- An ESD wrist strap with a plug for connection to the ESD connector on the MLX Series router.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

The MLXe-4 router ships with slot blanks installed in all empty module slots. The slot blanks help ensure proper airflow inside the router. You must remove the slot blank to install a module into a slot.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

NOTE
If you are hot-swapping a module, allow a minimum of two seconds after a module (or power supply or fan tray) has been removed before inserting a module in the same slot.

Although the slot blanks differ in size, the procedure for removing them is identical. You will need a flat-blade screwdriver to remove slot blanks.

Follow these steps to remove a slot blank.

1. Loosen the screws on either end of the slot blank by hand or with a flat-blade screwdriver.
2. Pull the slot blank out of the router, and store it in a safe place for future use.

   Follow these steps to install a module.

Installing power supplies in an MLXe-4 router

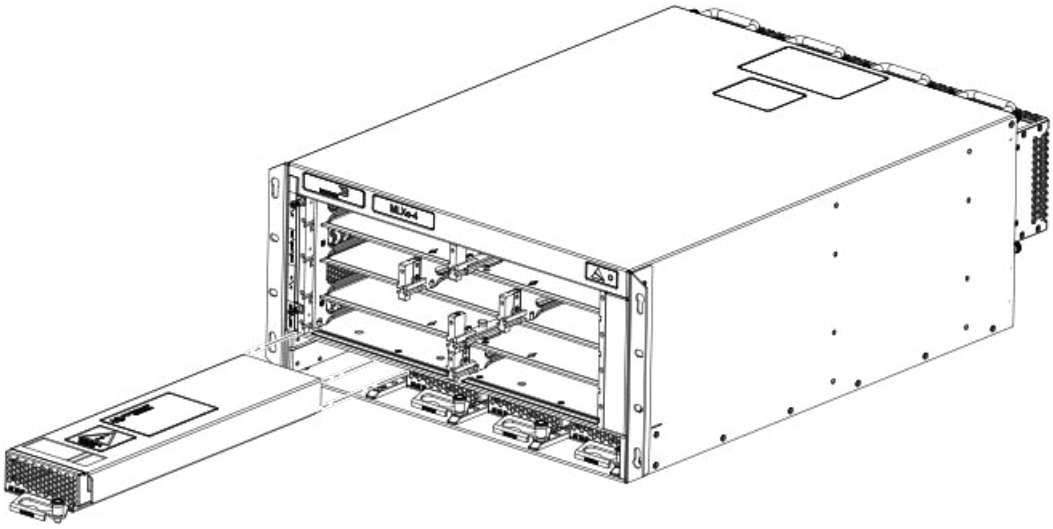
Follow these steps to install a power supply.

1. Remove the power supply slot blank and store it for future use.
2. Remove the power supply from the packaging.
3. Insert the power supply into the slot and slide it along the guides on each side of the slot., as shown in the following figure.

   CAUTION
   If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

   CAUTION
   Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

   FIGURE 30 Installing a power supply



4. Push the power supply front panel into the router until it engages the backplane connector, and the latch pin clicks into place.

   For information about connecting power to the router, refer to Connecting AC power on page 99.

Connecting AC power

AC power is supplied through a power cord connected to the AC power supply installed in the router.

NOTE
For the NEBS-compliant installation, AC power connections must use a surge protection device (SPD) to protect the AC power supplies from damage due to excessive power line surges.

Follow these steps to connect the AC power cord.

1. Locate the power supply AC inlet on rear of chassis for the associated installed power supply.
2. Lift the cord retainer and connect the AC power cord to the AC inlet.
3. Snap the cord retainer over the power plug to hold it in place.

DANGER
If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

For information about powering on the system, refer to Activating the power source on page 172.

Connecting DC power

You can provide DC power for the router by installing a DC-to-DC power supply. The DC-to-DC supply converts 48V-DC input from a power source to 12V-DC for your router.

DANGER
The procedures in this manual are for qualified service personnel.

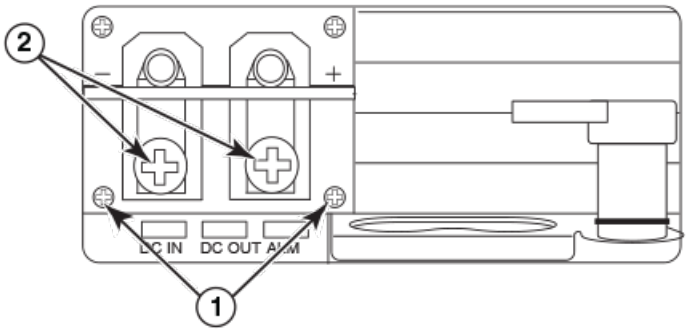
NOTE
Because there are multiple power supply vendors, the LED layout on your DC power supply may differ from what is shown in the following figure. However, the LED functions are identical.

NOTE
The 1200W and the 1800W power supplies are for use with the MLXe-4, MLXe-8, and MLXe-16 routers.

Follow these steps to connect a DC power source.

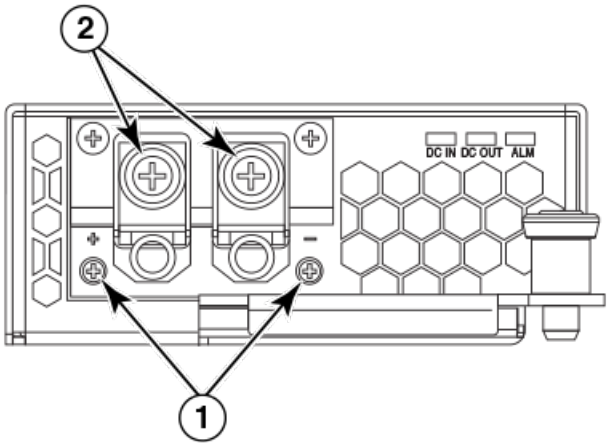
1. Use a #1 Phillips screwdriver to remove the two screws that hold the transparent cover over the power supply lugs, as shown in one of the two following figures (dependent on the power supply).

   FIGURE 31 The MLX Series DC 1200W power supply



   1. Screws holding transparent cover
   2. Power lug screws

   FIGURE 32 The MLX Series DC 1800W power supply



   1. Screws holding transparent cover
   2. Power lug screws

2. Use a #2 Phillips screwdriver to remove the power lugs.

3. Crimp #8 AWG power supply wire into the power lugs and reconnect the lugs to the power supply unit, as shown in the following figure.

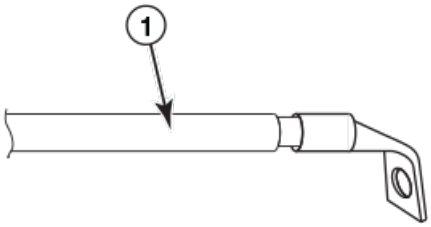
   For the NEBS-compliant installation of MLXe-4, MLXe-8 and MLXe-16 routers:

   CAUTION
   For an Extreme Networks AC system, use a ground wire of at least 6 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

   CAUTION
   For a DC system, use a grounding wire of at least 6 American Wire Gauge (AWG). The 6 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. For the Ground lug, use UL listed Panduit crimp connector, P/N LCD6-10A, and two 10-32, PPH, screws to secure crimp connector to chassis. Grounding position is located on the side of the chassis adjacent ground symbol.

   NOTE
   To ensure adequate bonding when attaching the ground lug, a minimum of 20 PSI of torque is required to be applied to the mounting hardware used to attach the ground lug.

   FIGURE 33 Crimping the power supply wire in the lug



   1. AWG power supply wire: #8 AWG power supply wire for 1200W power supplies#6 AWG power supply wire for 1800W power supplies

4. Connect the -48V cable to the negative terminal and the 0V cable to the positive terminal.

   NOTE
   DC return must be isolated from the router ground (DC-I) when connecting to DC power supplies.

5. Replace the transparent cover.

   This equipment installation must meet NEC/CEC code requirements. Consult local authorities for regulations.

Final steps

Complete these steps in the order listed:

1. Perform the step Attaching a management station on page 171.
2. Perform the step Activating the power source on page 172.
3. Perform the step Verifying proper operation on page 172.

Installing an MLX-8 router

This section describes how to install an MLX-8 router.

> NOTE
> Illustrations in this chapter may differ slightly from the actual equipment.

Preparing the installation site

Before installing the router, plan the location and orientation relative to other devices and equipment. For cooling purposes, allow a minimum of six inches of space between the sides, front, and the back of the router and walls or other obstructions. If a router is installed in a perforated enclosure, the perforations must cover at least 60 percent of the surface.

> NOTE
> This equipment is suitable for installation in a Network Telecommunication facility and where NEC requirements apply. Additionally, it may be installed in either a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). It is not intended for Outside Plant (OSP) installations.

Ensure that the proper cabling is installed at the site.

For information on cabling, refer to Installing power supplies in the MLXe-8 router on page 107, Attaching a management station on page 171, and Connecting the router to a network device on page 197.

Unpacking an MLXe-8 router

The MLXe-8 router ships with the following items:

- Switch fabric modules installed in slots marked SF, and slot blanks installed in all empty module slots.
- Two AC or two DC power supplies
- Insertion or extraction tool for use with RJ-45 and fiber-optic connectors.

Save the shipping carton and packing materials in case you need to move or ship the router at a later time.

Lifting guidelines for MLXe-8 routers

Follow these guidelines for lifting and moving MLXe-8 routers:

- Before lifting or moving the router, disconnect all external cables.
- Do not attempt to lift a fully configured router by yourself.
- It is recommended that you install router components after you have installed the router in a rack.

Installing an MLXe-8 router in an EIA rack

Because of the weight of a fully loaded MLXe-8 router, Extreme Networks recommends mounting it in a rack before installing the modules and AC power supplies.

You can install up to six MLXe-8 routers in a standard 19-inch (EIA310-D) rack using the standard rack installation method. If you use the EIA rack mounting kit, you can install up to 4 MLXe-8 routers in a standard 19-inch rack.

Front- or mid-mount your device in a standard rack

Your MLXe-8 router ships from the factory with mounting brackets attached for front-mount installation in a standard 2-post rack. You can also use these brackets for a mid-mount installation by simply removing the brackets from the front edges of the device and re-attaching them in the center sides of the device using the pre-drilled holes. Refer to Figure 35.

You will need to provide four standard #12-24 pan-head screws (per router) and a #2 Phillips screwdriver to secure routers in the rack.

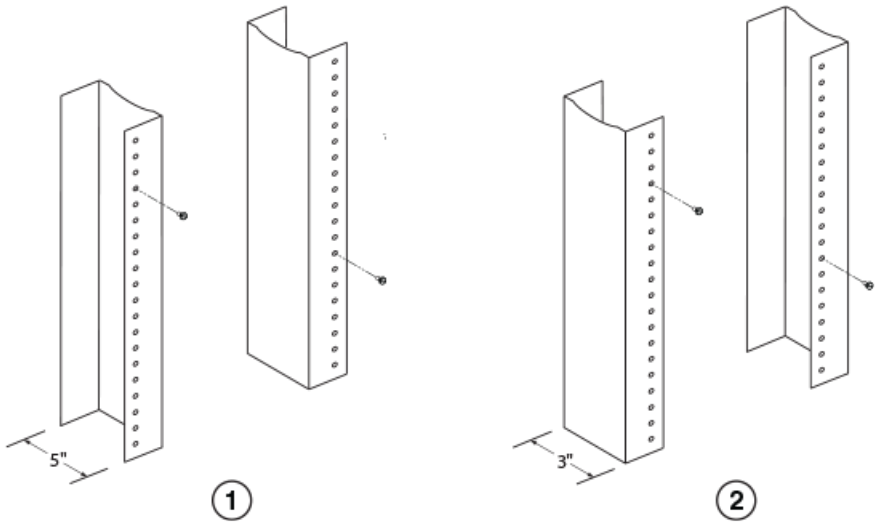
If you are installing your MLXe-8 router in a cabinet or 4-post rack, refer to Installing MLXe-4 and MLXe-8 routers in a 4-post EIA rack on page 121.

> **NOTE**
> When connecting the device to the rack frame, use thread-forming screws and paint-piercing washers.

Follow these steps to mount your device in a standard 2-post rack in either a front- or mid-mount configuration.

1. Determine the position of each router in the rack according to weight. For example, mount the router with the fewest modules near the top of the rack, the router with more modules near the middle of the rack, and a fully populated router near the bottom of the rack.
2. Using the keyhole slots in the router mounting brackets as a guide, align one screw per rack post, as shown in the following figure. On one side of the rack, the screw should align with the top hole in the mounting bracket. On the other side of the rack, the screw should align with the bottom hole of the mounting bracket. When tightening these screws, leave approximately 1/4 inch of clearance between the back of the screw head and the rack post.

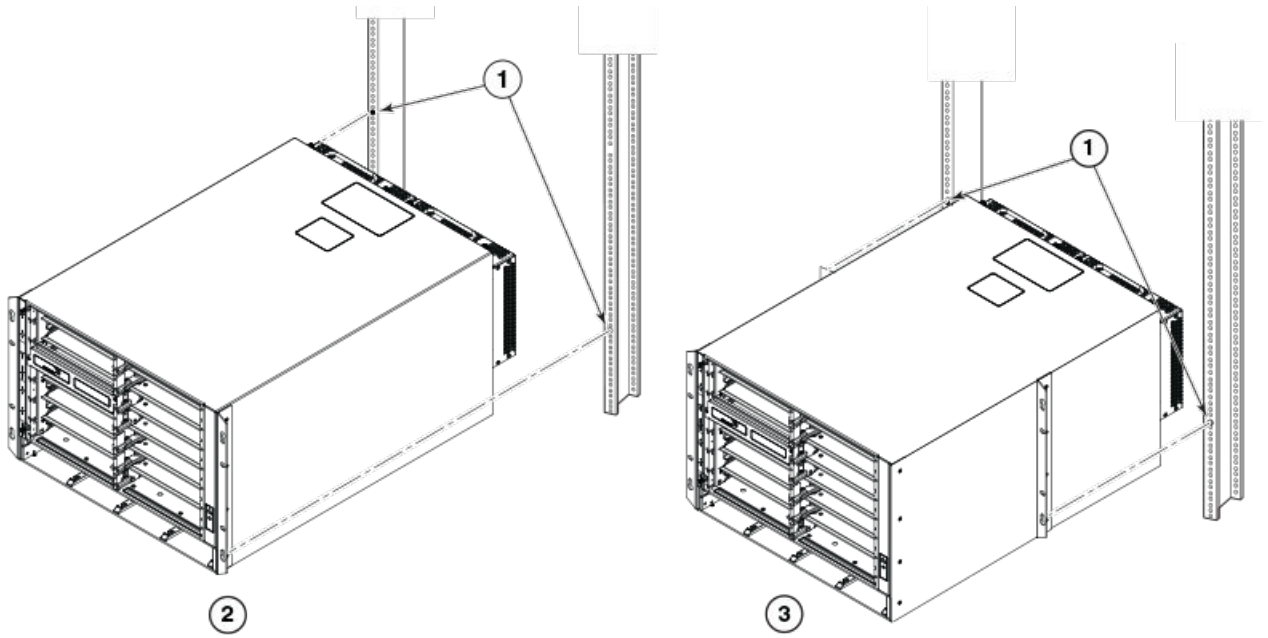
FIGURE 34 Positioning the mounting screws in rack posts



1. Unequal flange equipment rack
2. Network equipment rack

3. Mount the lowest router first. With one person on each side, lift the router and slip the widest part of each keyhole slot on the mounting bracket over the corresponding screw in the rack post, as shown in the following figure.

FIGURE 35 Mounting the router in a rack



1. Screws in mounting posts
2. Front-mount position installation
3. Mid-mount installation

4. Slide the router down so that the mounting screw heads are in the narrowest part of the keyhole slots.
5. Tighten the screws to secure the router in place. For extra support, use additional screws.

NOTE
For better grounding of the router to the rack, attach the router using star washers. You should also use star washers with any single-hole grounding lugs to keep the lugs from rotating.

Repeat step 2 through step 5 to mount each router in the rack, moving from lowest to highest.

Installing the MLXe-8 router modules

The sequence for installing multiple modules is important to ensure proper fit. The recommended sequence for the MLXe-8 router is to install right-to-left, beginning with the lowest row and moving up.

The MLXe-8 router ships with the required switch fabric modules installed.

For instructions about installing 2x100GbE interface modules, refer to Installing 2x100GbE CFP2 interface modules on page 91.

For instructions about installing BR-MLX-10Gx24-DM interface modules, refer to Installing BR-MLX-10Gx24-DM interface modules on page 92.

NOTE
Installation instructions are identical for interface, management, and switch fabric modules.

DANGER
The intra-building port or ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port or ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 5) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

NOTE
MLX Series router modules are dedicated, which means that you must install them in the MLX Series router only. If you try to install a MLX Series router module in a non- MLX Series router, or install a module intended for a non- MLX Series router in a MLX Series router, the router and module will not function properly.Although management modules are designed to be hot-swappable, you must upgrade the software on all interface modules and management modules to the appropriate software release before installing them. For more information on the appropriate software release, refer to the Hardware Installation Notes that shipped with the management module.

The following table identifies the router slot numbers where the modules must be installed. An identifying label can be seen at the base of each slot.

TABLE 29 MLX-8 router module slot designations

Module	Slot number
Management modules	Active module - M1 (left).Redundant module - M2 (right).
Interface modules	1 - 8
Switch fabric modules	SF1 - SF3

For information about how to disable and re-enable power to interface modules, refer to Disabling and re-enabling power to interface modules on page 224.

If you are installing a redundant management module, refer to the chapter titled "Using a Redundant Management Module" in the MLX Series *and Extreme NetIron Family Configuration Guide* for information about how the redundant module works, optional software configurations, and how to manage redundancy.

Before installing a module in the MLXe-8 router, have the following items available:

- A large flat-blade screwdriver.
- An ESD wrist strap with a plug for connection to the ESD connector on the router.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

You can install modules while the router is powered on and running.

The router ships with slot blanks installed in all empty module slots. The slot blanks help ensure proper airflow inside the router. You must remove the slot blank to install a module.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

Although the slot blanks differ in size, the procedure for removing them is identical. You will need a flat-blade screwdriver to perform this task.

Follow these steps to remove a slot blank.

1. Loosen the screws on either end of the slot blank by hand or with a flat-blade screwdriver.
2. Pull the slot blank out of the router, and store it in a safe place for future use.

> **NOTE**
> If you are hot-swapping a module, allow a minimum of two seconds after a module (or power supply or fan tray) has been removed before inserting a module in the same slot.

Follow this procedure to install a module in the router.

Installing power supplies in the MLXe-8 router

Follow these steps to install a power supply in the MLXe-8 router.

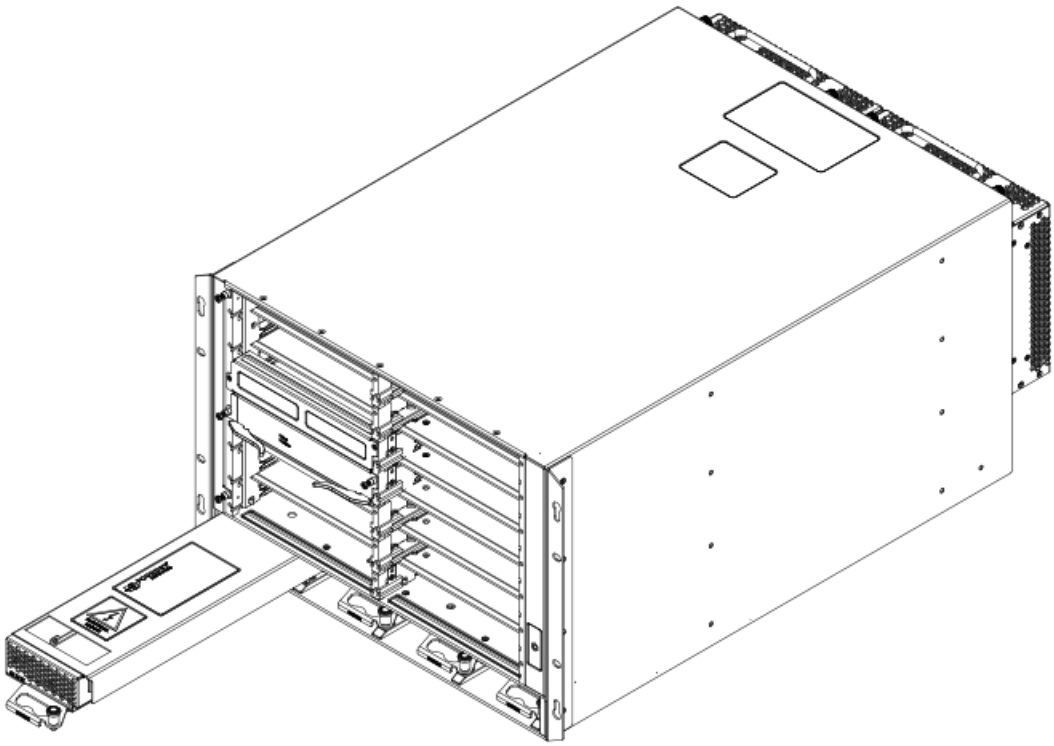
1. Remove the power supply slot blank.
2. Remove the power supply from the packaging.

3. Insert the power supply into the slot and slide it along the guides on each side of the slot, as shown in the following figure.

   CAUTION
   If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

   CAUTION
   Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

   FIGURE 36 Installing a power supply in an MLXe-8 router



4. Push the power supply front panel into the router until it engages the backplane connector, and the latch pin clicks into place.

   For information about connecting power to the router, refer to Connecting AC power on page 108, or Connecting DC power on page 100.

Connecting AC power

AC power is supplied through the power cord that is connected to the AC power supply in the router.

NOTE
For the NEBS-compliant installation, AC power connections must use a surge protection device (SPD) to protect the AC power supplies from damage due to excessive power line surges.

Follow these steps to connect the AC power cord.

1. Locate the AC inlet on rear of chassis for the associated installed AC power supply.

2. Lift the cord-retainer and connect the AC power cord to the associated power supply AC inlet.
3. Snap the cord-retainer over the power plug to hold it in place.

   Follow these steps to connect the AC power cord.

   DANGER
   If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

   For information about powering on the system, refer to Activating the power source on page 172.

Connecting DC power

You can provide DC power for the router by installing a DC-to-DC power supply. The DC-to-DC supply converts 48V-DC input from a power source to 12V-DC for your router.

DANGER
The procedures in this manual are for qualified service personnel.

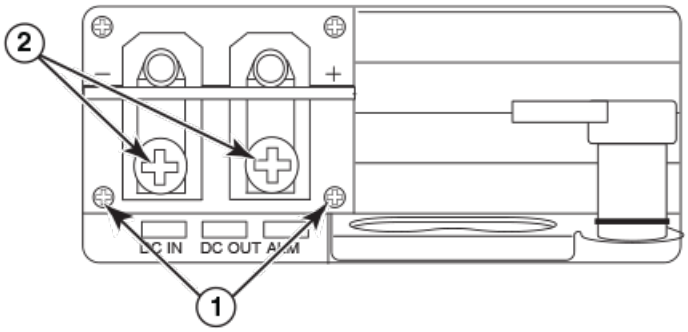
NOTE
Because there are multiple power supply vendors, the LED layout on your DC power supply may differ from what is shown in the following figure. However, the LED functions are identical.

NOTE
The 1200W and the 1800W power supplies are for use with the MLXe-4, MLXe-8, and MLXe-16 routers.

Follow these steps to connect a DC power source.

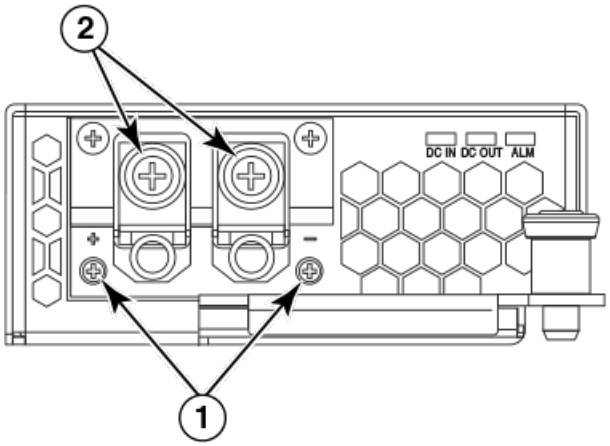
1. Use a #1 Phillips screwdriver to remove the two screws that hold the transparent cover over the power supply lugs, as shown in one of the two following figures (dependent on the power supply).

   FIGURE 37 The MLX Series DC 1200W power supply



   1. Screws holding transparent cover
   2. Power lug screws

   FIGURE 38 The MLX Series DC 1800W power supply



   1. Screws holding transparent cover
   2. Power lug screws

2. Use a #2 Phillips screwdriver to remove the power lugs.

3. Crimp #8 AWG power supply wire into the power lugs and reconnect the lugs to the power supply unit, as shown in the following figure.

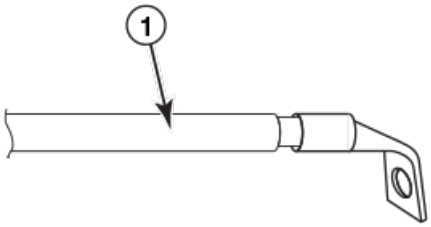
   For the NEBS-compliant installation of MLXe-4, MLXe-8 and MLXe-16 routers:

   CAUTION
   For an Extreme Networks AC system, use a ground wire of at least 6 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

   CAUTION
   For a DC system, use a grounding wire of at least 6 American Wire Gauge (AWG). The 6 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. For the Ground lug, use UL listed Panduit crimp connector, P/N LCD6-10A, and two 10-32, PPH, screws to secure crimp connector to chassis. Grounding position is located on the side of the chassis adjacent ground symbol.

   NOTE
   To ensure adequate bonding when attaching the ground lug, a minimum of 20 PSI of torque is required to be applied to the mounting hardware used to attach the ground lug.

   FIGURE 39 Crimping the power supply wire in the lug



   1. AWG power supply wire: #8 AWG power supply wire for 1200W power supplies#6 AWG power supply wire for 1800W power supplies

4. Connect the -48V cable to the negative terminal and the 0V cable to the positive terminal.

   NOTE
   DC return must be isolated from the router ground (DC-I) when connecting to DC power supplies.

5. Replace the transparent cover.

   This equipment installation must meet NEC/CEC code requirements. Consult local authorities for regulations.

Final steps

Complete these final steps in the order listed:

1. Perform the step Attaching a management station on page 171.
2. Perform the step Activating the power source on page 172.
3. Perform the step Verifying proper operation on page 172.

Installing an MLXe-16 router

The following sections describe how to install an MLXe-16 router.

> NOTE
> Illustrations may differ slightly from the actual equipment.

Preparing the installation site

Before installing the router, plan the location and orientation relative to other devices and equipment. For cooling purposes, allow a minimum of six inches of space between the sides, front, and the back of the router and walls or other obstructions. If you are installing the router in a perforated enclosure, the perforations must cover at least 60 percent of the surface.

Ensure that the proper power and network cabling is installed at the site. For information about cabling, refer to Installing power supplies in the MLXe-16 router on page 117,and Attaching a management station on page 171.

> NOTE
> This equipment is suitable for installation in a Network Telecommunication facility and where NEC requirements apply. Additionally, it may be installed in either a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). It is not intended for Outside Plant (OSP) installations.

Unpacking an MLXe-16 router

The MLXe-16 router ships with the following items:

- Router chassis with switch fabric modules installed in the slots marked SF, and slot blanks installed in all empty module slots.
- Four AC or four DC power supplies
- Insertion or extraction tool for use with RJ-45 and fiber-optic connectors.

If any of these items are missing, contact the place of purchase.

Remove your MLXe-16 router from the shipping carton. Save the shipping carton and packing materials in case you need to move or ship the router at a later time.

Lifting guidelines for the MLXe-16 routers

> DANGER
> ***A fully populated chassis is heavy. TWO OR MORE PEOPLE ARE REQUIRED WHEN LIFTING, HANDLING, OR MOUNTING THESE DEVICES.***

Follow these guidelines for lifting and moving your MLXe-16 router:

- Before lifting or moving the router, disconnect all external cables.
- Do not attempt to lift a fully configured router by yourself. Use two people to lift the router.
- It is recommended that you remove router components before installing the router in a rack.

Installing an MLXe-16 router in an EIA rack

DANGER
Make sure the rack housing the device is adequately secured to prevent it from becoming unstable or falling over.

DANGER
Mount the devices you install in a rack as low as possible. Place the heaviest device at the bottom and progressively place lighter devices above.

You can install your router in a standard rack in either a front- or mid-mount position using the factory-installed mounting brackets. For a mid-mount configuration, simply remove the mounting brackets from the front edges of the device and re-attach them using the pre-drilled holes in the center sides of the device.

You can install up the three MLXe-16 routers in a standard 19-inch (EIA310-D) rack.

If you are installing your MLXe-16 router in a 4-post EIA rack, refer to Installing a MLXe-16 router in a 4-post EIA rack on page 128.

Front- or mid-mount in a standard rack

Follow these steps to mount an MLXe-16 router in a rack.

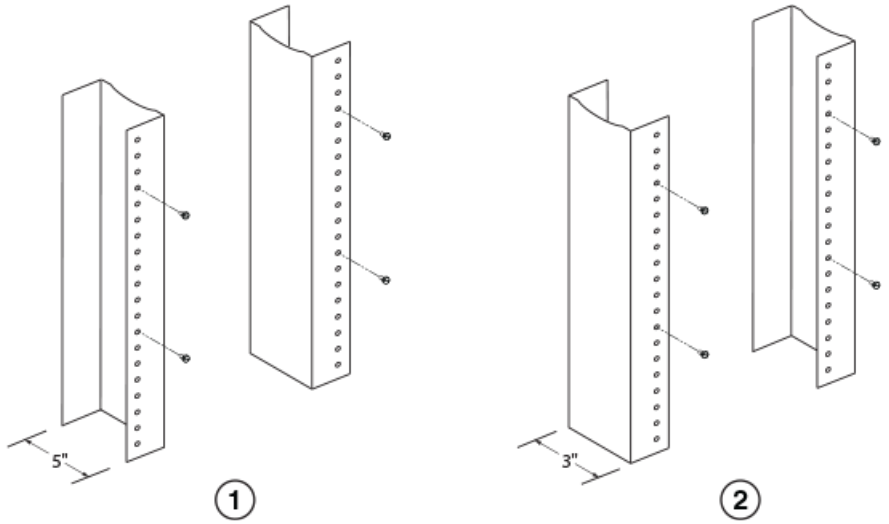
You will need to provide standard #12-24 pan-head screws to mount each router in a rack. You will need a Phillips screwdriver to perform this task.

NOTE
When connecting the device to the rack frame, use thread-forming screws and paint-piercing washers.

1. Determine the position of each router in the rack. For example, place routers with the fewest modules near the top of the rack, routers with more modules near the middle of the rack, and fully populated routers near the bottom of the rack.

2. Position four mounting screws for each router using the spacing of the keyhole slots (the ones with the narrow portion pointing up) on the mounting brackets as a guide, as shown in the following figure. When tightening the mounting screws, leave approximately 1/4 inch of clearance between the back of the screw head and the rack posts.

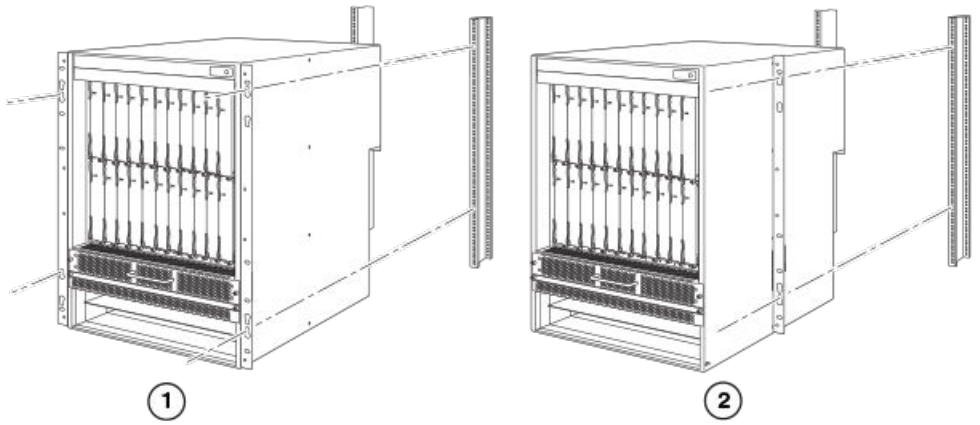
FIGURE 40 Positioning the mounting screws in the rack posts



1. Unequal flange equipment rack
2. Network equipment rack

3. Starting with the router that will be in the lowest position in the rack, mount the router in the rack as shown in the following figure. With two or more people lifting the router, slip the wide portion of each keyhole slot over the corresponding mounting screw in the rack post.

FIGURE 41 Mounting the MLXe-16 router in a rack



1. Front-mount configuration
2. Mid-mount configuration

4. Slide the router down so that the mounting screw heads are in the narrow portion of the keyhole slots.

5. Tighten the screws to secure the router in place. For extra support, use additional screws.

   NOTE
   For better grounding of the router to the rack, attach the router using star washers. You should also use star washers with any single-hole grounding lugs to keep the lugs from rotating.

   NOTE
   When making the primary ground connection, use a star washer to prevent lug rotation.

Repeat step 2 through step 5 to mount each router in the rack.

Installing the MLXe-16 router modules

The MLXe-16 router ships with the required switch fabric modules installed.

The installation sequence for multiple modules is important to ensure proper fit. Always fill the bottom slots in the MLXe-16 router first. Begin by filling the slots from the left side of the router, and work towards the right side. Refer to MLXe-16 router components on page 23 for slot locations.

NOTE
Installation instructions are identical for interface, management, and switch fabric modules. However, there are specific requirements and installation instructions for the following devices: For installing NI-MLX-1Gx48-T-A modules in the MLXe-16 router., refer to the high-speed fan and software requirements documented in NIBI-16-FAN-EXH-A high-speed fan assemblies on page 86 and NI-MLX-1Gx48-T-A interface module on page 69. For installing 2x100GbE interface modules, refer to Installing 2x100GbE CFP2 interface modules on page 91.For instructions about installing BR-MLX-10Gx24-DM interface modules, refer to Installing BR-MLX-10Gx24-DM interface modules on page 92.

DANGER
The intra-building port or ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port or ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 5) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

Router slot numbers into which you must install the modules are shown in the following table. Markings for the router slots appear at the base of the slots.

TABLE 30 MLXe-16 module slot designations

Module	Slot number
Management modules	Active module - M1 (upper).Redundant module - M2 (lower).
Interface modules	1 - 16
Switch Fabric modules	SF1 - SF4

NOTE
If you are installing a redundant management module, refer the *Extreme NetIron Management Configuration Guide* for information about how the redundant module works, optional software configurations that you can perform, and how to manage the redundancy feature.

NOTE
MLX Series router modules are dedicated, which means that you must install them in MLX Series routers only. If you install a MLX Series module in another Extreme router or install a module intended for another Extreme router in an MLX Series router, the router and module may not function properly. Even though management modules are designed to be hot-swappable, you must upgrade the software on all interface modules and management modules to the appropriate Extreme NetIron software release before installing them. For more information on the appropriate software release, refer to the Hardware Installation Notes that shipped with the management module.

For information about how to disable and re-enable power to interface modules, refer to Disabling and re-enabling power to interface modules on page 224.

Before installing modules in the MLXe-16 router, have the following items available:

- A large flat-blade screwdriver.
- A new or replacement interface module, which you can order from Extreme Networks.
- An ESD wrist strap with a plug to attach to the ESD connector on the router chassis.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

NOTE
Use of a power screwdriver may twist the heads from the screws and is not recommended.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

Reset fan speed to auto

For MLXe-16 routers, if you insert a module into a slot where the fan speed for a previous module was manually configured, you will need to change the fan speed back to auto. For example, if the fan speed was manually configured to "slow", and you are installing a module that requires more cooling power, the "slow" setting will cause the module to overheat. To configure the fan speed to auto, enter the following command:

device `# set-fan-speed auto`

The MLXe-16 router ships with slot blanks installed in all empty module slots. The slot blanks help ensure proper airflow inside the router. You must remove the slot blank to install a module in a slot.

Although the slot blanks differ in size, the procedure for removing them is identical. You will need a flat-blade screwdriver to perform this task.

Follow these steps to remove a slot blank.

1. Loosen the screws on either end of the slot blank by hand or with a flat-blade screwdriver.
2. Pull the slot blank out of the router and store it in a safe place for future use.

NOTE
If you are hot-swapping a module, allow a minimum of two seconds after a module (or power supply or fan tray) has been removed before inserting a module in the same slot.

Follow this procedure to install modules in the router.

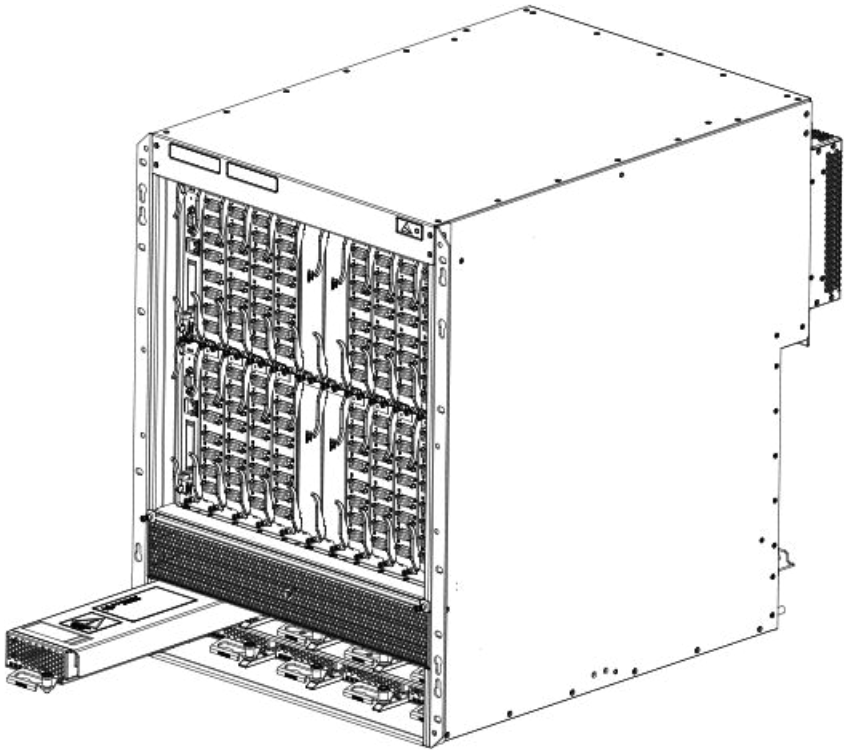
Installing power supplies in the MLXe-16 router

DANGER
High Touch Current. Earth connection essential before connecting supply.

Follow these steps to install a power supply in an MLXe-16 router.

1. Remove the power supply slot blank.
2. Remove the power supply from the packaging.
3. Insert the power supply into the slot, using the guides on either side of the slot. Refer to the following figure.

FIGURE 42 Installing a power supply in an MLXe-16 router



CAUTION
Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

4. Push the power supply front panel toward the back of the router. This action causes the power supply connector to engage the backplane connector.

   NOTE
   Do not over tighten screws when installing power supplies.

5. For information about connecting power to the router, refer to Connecting AC power on page 118.
6. For information about powering on the system, refer to Activating the power source on page 172.

Connecting AC power

NOTE
For the NEBS-compliant installation, AC power connections must use a surge protection device (SPD) to protect the AC power supplies from damage due to excessive power line surges.

AC power is supplied through a power cord connected to the power supply in the MLXe-16 router.

Follow these steps to connect AC power:

1. Locate the power supply AC inlet at the bottom rear of chassis for the associated installed power supply.
2. Lift the cord retainer and connect an AC power cord to the associated power supply AC inlet.
3. Snap the cord retainer over the power plug to hold it in place.

DANGER
If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

4. For information about powering on the system, refer to Activating the power source on page 172.

Connecting DC power

You can provide DC power for the router by installing a DC-to-DC power supply. The DC-to-DC supply converts 48V-DC input from a power source to 12V-DC for your router.

DANGER
The procedures in this manual are for qualified service personnel.

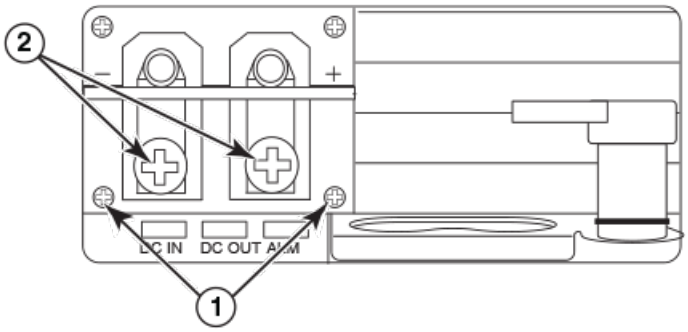
NOTE
Because there are multiple power supply vendors, the LED layout on your DC power supply may differ from what is shown in the following figure. However, the LED functions are identical.

NOTE
The 1200W and the 1800W power supplies are for use with the MLXe-4, MLXe-8, and MLXe-16 routers.

Follow these steps to connect a DC power source.

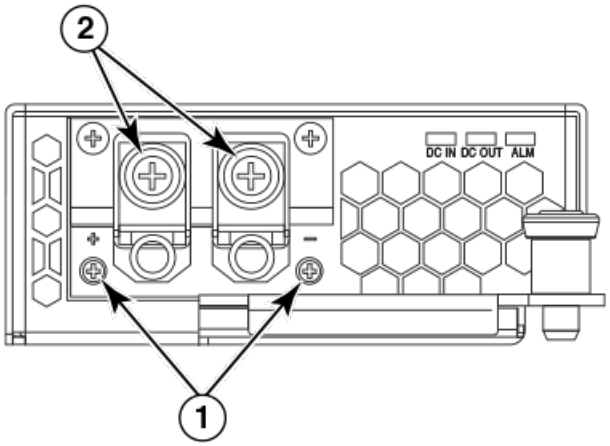
1. Use a #1 Phillips screwdriver to remove the two screws that hold the transparent cover over the power supply lugs, as shown in one of the two following figures (dependent on the power supply).

   FIGURE 43 The MLX Series DC 1200W power supply



1. Screws holding transparent cover	2. Power lug screws

   FIGURE 44 The MLX Series DC 1800W power supply



1. Screws holding transparent cover	2. Power lug screws

2. Use a #2 Phillips screwdriver to remove the power lugs.

3. Crimp #8 AWG power supply wire into the power lugs and reconnect the lugs to the power supply unit, as shown in the following figure.

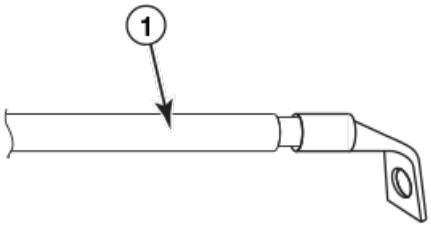
   For the NEBS-compliant installation of MLXe-4, MLXe-8 and MLXe-16 routers:

   CAUTION
   For an Extreme Networks AC system, use a ground wire of at least 6 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

   CAUTION
   For a DC system, use a grounding wire of at least 6 American Wire Gauge (AWG). The 6 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. For the Ground lug, use UL listed Panduit crimp connector, P/N LCD6-10A, and two 10-32, PPH, screws to secure crimp connector to chassis. Grounding position is located on the side of the chassis adjacent ground symbol.

   NOTE
   To ensure adequate bonding when attaching the ground lug, a minimum of 20 PSI of torque is required to be applied to the mounting hardware used to attach the ground lug.

   FIGURE 45 Crimping the power supply wire in the lug



   1. AWG power supply wire: #8 AWG power supply wire for 1200W power supplies#6 AWG power supply wire for 1800W power supplies

4. Connect the -48V cable to the negative terminal and the 0V cable to the positive terminal.

   NOTE
   DC return must be isolated from the router ground (DC-I) when connecting to DC power supplies.

5. Replace the transparent cover.

   This equipment installation must meet NEC/CEC code requirements. Consult local authorities for regulations.

Final steps

Complete these steps in the order listed:

- Perform the step Attaching a management station on page 171.
- Perform the step Activating the power source on page 172.
- Perform the step Verifying proper operation on page 172.

Mounting the MLX-4, MLX-8 or MLX-16 router in a 4-post rack or EIA rack

EIA rack or 4-Post Rack Mount Kit contents

You can mount MLX Series routers in a EIA rack or 4-post rack using the optional EIA rack/4-post rack mount kits available from Extreme Networks. The following table lists these kits and their contents.

TABLE 31 EIA rack/4-Post Rack Mount Kits for MLXe-4, MLXe-8, and MLXe-16 routers

Contents for RMK-CAB-MLXE-4	Contents for RMK-CAB-MLXE-8	Contents for RMK-CAB-MLXE-16
Front bracket left A (1)	Front bracket left A (1)	Front bracket left A (1)
Front bracket right B (1)	Front bracket right B (1)	Front bracket right B (1)
Left side plate A (1)	Left side plate A (1)	Left side plate A (1)
Right side plate (B 1)	Right side plate B (1)	Right side plate B (1)
2U shelf assembly (1)	2U shelf assembly (1)	Chassis alignment rail ((1)
Adjustable top rail (1)	Adjustable top rail (1)	Air block shelf (1)
Rail extender for top rail, 27-29" (1)	Rail extender for top rail, 27-29" (1)	Phillips flat-head screws, 6-32x1/4" (10)
Rail extender for top rail, 29-31" (1)	Rail extender for top rail, 29-31" (1)	Snap plastic rivets (12)
Thermal duct (1)	Thermal duct (1)	Right transport bracket, 27-29" (1)
Right transport bracket, 27-29" (1)	Right transport bracket, 27-29" (1)	Left transport bracket, 27-29" (1)
Left transport bracket, 27-29" (1)	Left transport bracket, 27-29" (1)	Right transport bracket, 29-31" (1)
Right transport bracket, 29-31" (1)	Right transport bracket, 29-31" (1)	Left transport bracket, 29-31" (1)
Left transport bracket, 29-31" (1)	Left transport bracket, 29-31" (1)	Alignment washers (4)
Alignment washers (4)	Alignment washers (4)	Phillips pan-head screws, 10-32x.63", square cone (30)
Phillips pan-head screws, 10-32x.63", square cone (30)	Phillips pan-head screws, 10-32x.63", square cone (30)	Floating clip nut, 10-32 (26)
Floating clip nut, 10-32 (26)	Floating clip nut, 10-32 (26)	Retainer nut, 10-32 (26)
Retainer nut, 10-32 (26)	Retainer nut, 10-32 (26)	Screws, 6-32, 1/4" Phillips flat-head, zinc, black (18)
Snap plastic rivets (12)	Snap plastic rivets (12)	Screws, 10-32, 1/4" Phillips flat-head, 100Deg, steel, black (16)
Phillips flat-head screws, 6-32x1/4" (10)	Phillips flat-head screws, 6-32x1/4" (10)	
Screws, 6-32, 1/4" Phillips flat-head, zinc, black (18)	Screws, 6-32, 1/4" Phillips flat-head, zinc, black (18)	
Screws, 10-32, 1/4" Phillips flat-head, 100Deg, steel, black (16)	Screws, 10-32, 1/4" Phillips flat-head, 100Deg, steel, black (16)	

Installing MLXe-4 and MLXe-8 routers in a 4-post EIA rack

This section describes how to install MLXe-4 or MLXe-8 routers in a 4-post EIA rack using the RMK-CAB-MLXE-4 or RMK-CAB-MLXE-8 4-Post Rack Mount Kits.

To install an MLXe-16 router, use the RMK-CAB-MLXE-16 4-Post Rack Mount Kit, and refer to Installing a MLXe-16 router in a 4-post EIA rack on page 128.

NOTE
Because of the weight of fully loaded routers, it is recommended that you mount the router in an EIA rack before installing modules and power supplies.

You can install up to six MLX-4 routers in an EIA rack using the RMK-CAB-MLXE-4 4-Post Rack Mount Kit. You can install up to four MLXe-8 routers in an EIA rack using the RMK-CAB-MLXE-8 4-Post Rack Mount Kit.

Many of the parts in these rack mount kits can be adjusted to accommodate a variety of EIA rack configurations.

Mounting your MLX Series router in a 4-post EIA rack

Follow these steps to mount each MLXe-4 or MLXe-8 router in an EIA rack using the 4-Post EIA rack Mount Kit, starting with the lowest device first.

The kits contain a variety of screws, nuts, clip nuts, and washers, for use in the following ways:

- Use floating clip nuts in EIA racks with round holes.
- Use retainer nuts in EIA racks with square holes.
- Use the square alignment washers for both round and square holes.

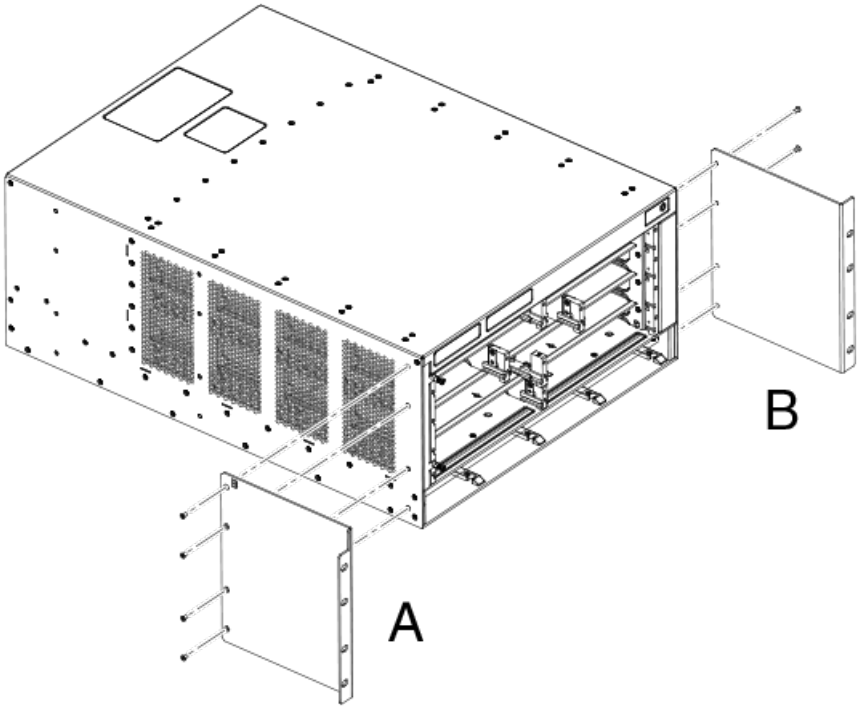
Select the appropriate hardware for your EIA rack configuration.

1. Place routers in the rack according to their weight. For example, mount the router with the fewest modules near the top of the rack, a router with more modules near the middle of the rack, and a fully populated router near the bottom of the rack.
2. Remove the factory-installed mounting brackets from the chassis.

3. Attach the front mounting brackets to the chassis using eight 6-32 flat head screws.

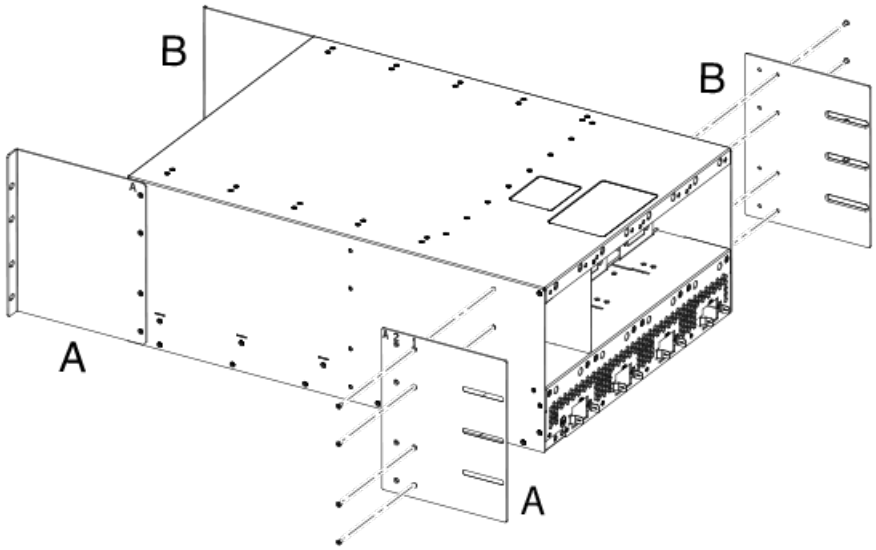
   Brackets are marked with A or B. As you face the front of the EIA rack, A brackets must be installed on the left side, and B brackets are installed on the right side. Do not mix A and B brackets. Refer to the following figure. The process is identical for 4-slot and 8-slot routers.

   FIGURE 46 Attach front mounting brackets to the router (MLXe-4 router shown)



4. Attach the side plates A and B to the rear of the router, using eight 6-32 flat-head screws, as shown in the following figure.

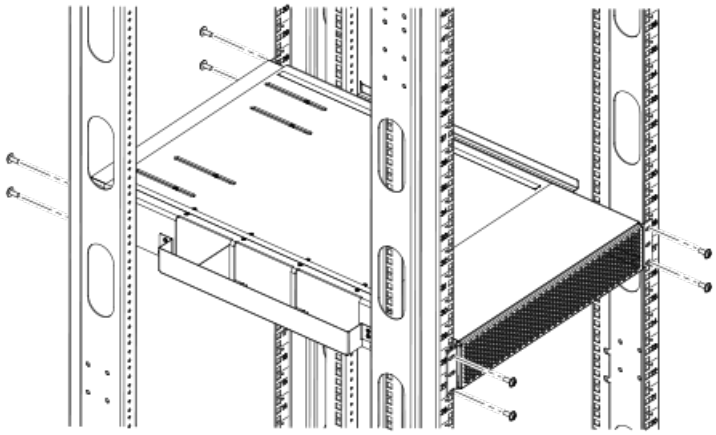
   FIGURE 47 Attach side plates to the rear of the router (MLXe-4 router shown)



   NOTE
   There are two sizes of side plates to accommodate EIA racks with depths of 27-28 inches, and depths of 29-31 inches. Be sure to select the side plate that is appropriate for your EIA rack.

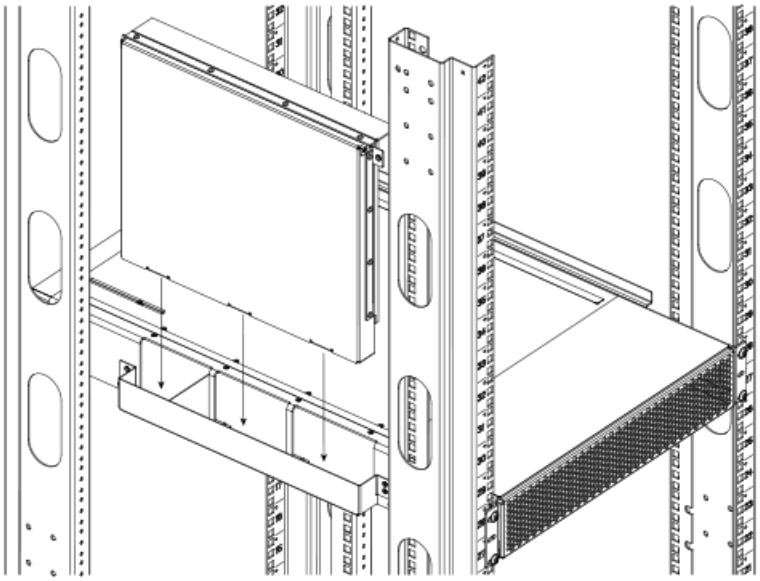
5. The mounting shelf adjusts to accommodate racks with depths from 27 to 31 inches, for both 4-slot and 8-slot routers. Slide the adjustable rails to the proper depth for your installation, and Install the mounting shelf to the rack rails using eight 10-32 screws, as shown in the following figure.

   FIGURE 48 Install the mounting shelf in the rack



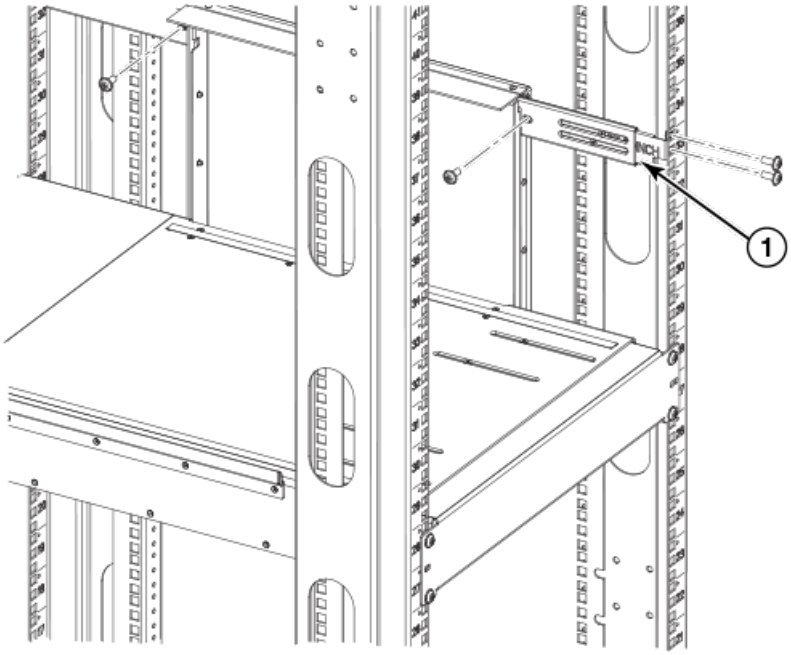
6. Install the side duct to the mounting shelf, using the tab and slot features at the base of the duct assembly. Refer to Figure 49.

FIGURE 49 Install side air ducts to the mounting shelf (MLXe-4 and MLXe-8 routers)



7. Select the rail extender that is appropriate for the depth of your EIA rack and attach it to the front of the top rail. Install the top rail to the EIA rack rails using four 10-32 screws. Attach the top rail to the duct assembly using two 6-32 flat-head screws, as shown in the following figure.

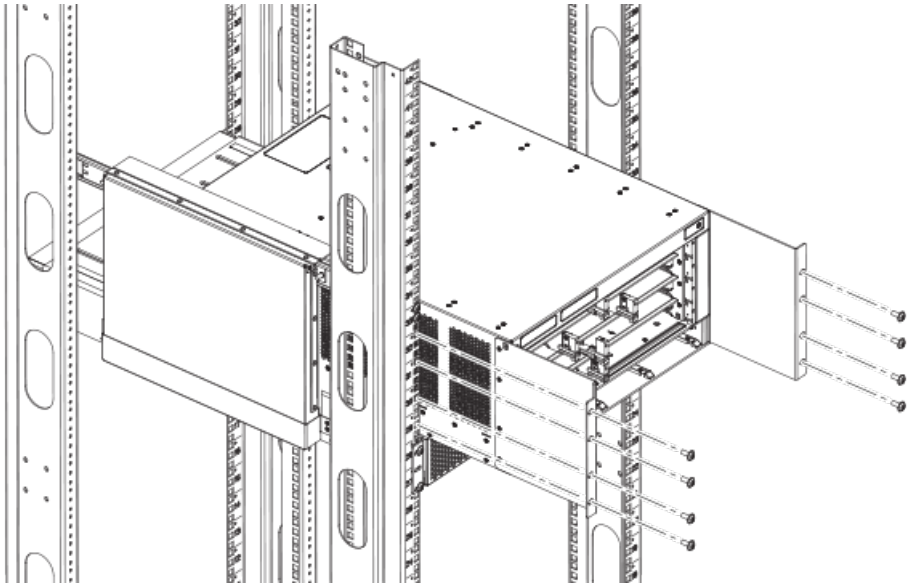
FIGURE 50 Install top rails to the rack



1	Rail extender

8. Install the router in the EIA rack. The router slides into the rack on top of the mounting shelf. Secure the router to the rack rails using eight 10-32 screws. Refer to the following figure (MLXe-4 router shown).

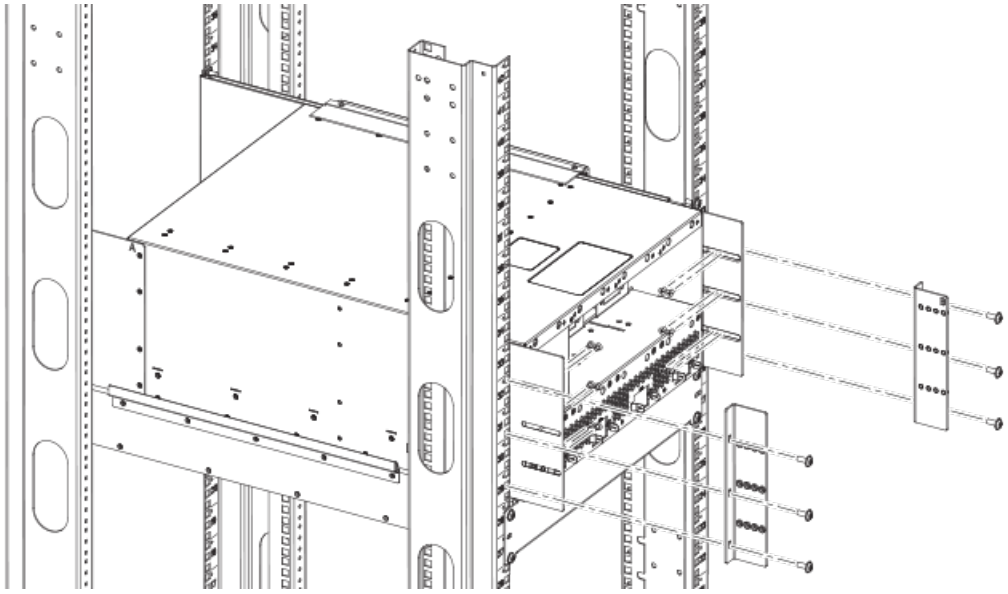
FIGURE 51 Install the router on the mounting shelf



9. Install the transport brackets to the EIA rack rails and to the side plates on the router, using six 10-32 screws, as shown in the following figure.

   NOTE
   The transport brackets provide extra stability, and must be installed if you plan to ship the device while it is mounted in the EIA rack. Before you install the transport brackets, you must first remove any installed fans.

   FIGURE 52 Attach transport brackets to router and to EIA rack



Installing a MLXe-16 router in a 4-post EIA rack

Using the 4-Post Rack Mount Kit, you can install up to four MLXe-16 routers in an EIA rack.

DANGER
Make sure the rack housing the device is adequately secured to prevent it from becoming unstable or falling over.

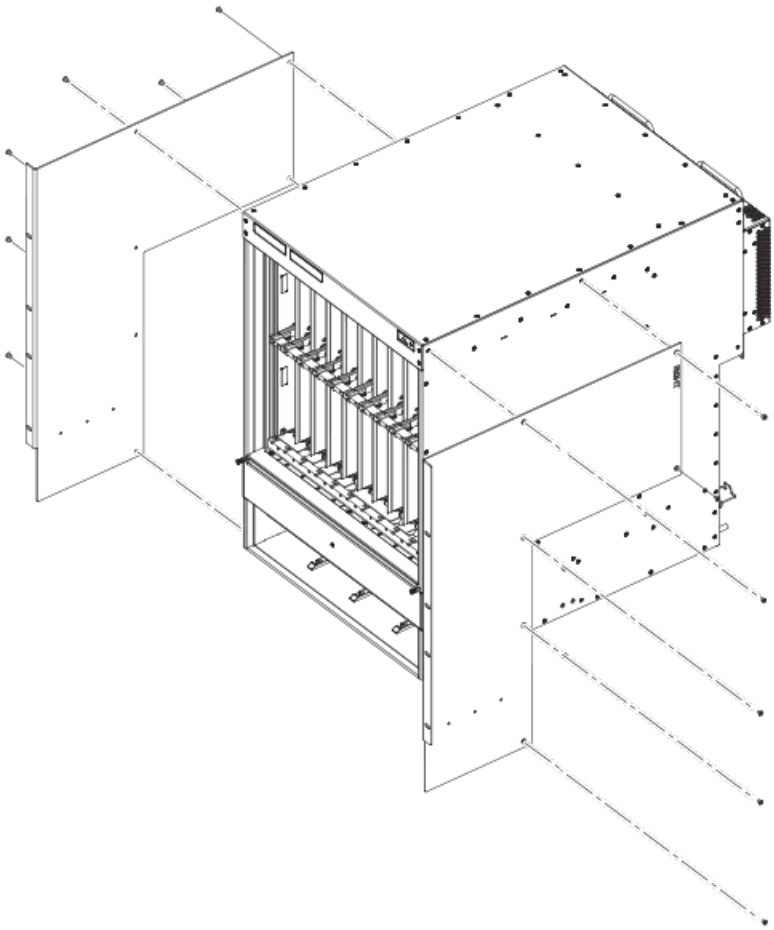
DANGER
Mount the devices you install in a rack as low as possible. Place the heaviest device at the bottom and progressively place lighter devices above.

To install your MLXe-16 router in a 4-post EIA rack, perform the following steps.

1. Remove the factory-installed mounting brackets from the sides of the router.

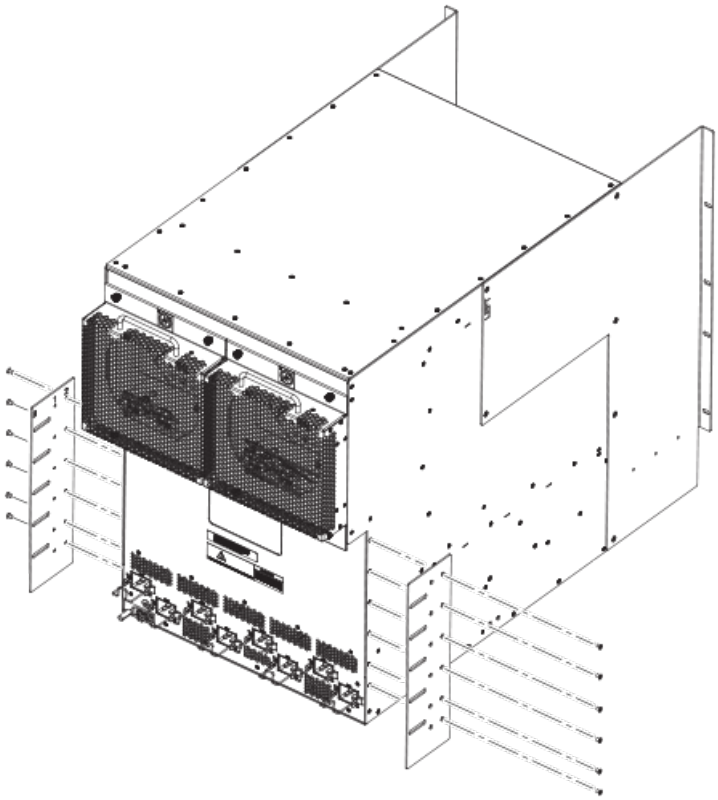
2. Attach the EIA rack mounting brackets to the front of the router using the 12 8-32 flat head screws, as shown in the following figure.

FIGURE 53 Attach the mounting brackets to the front of the router



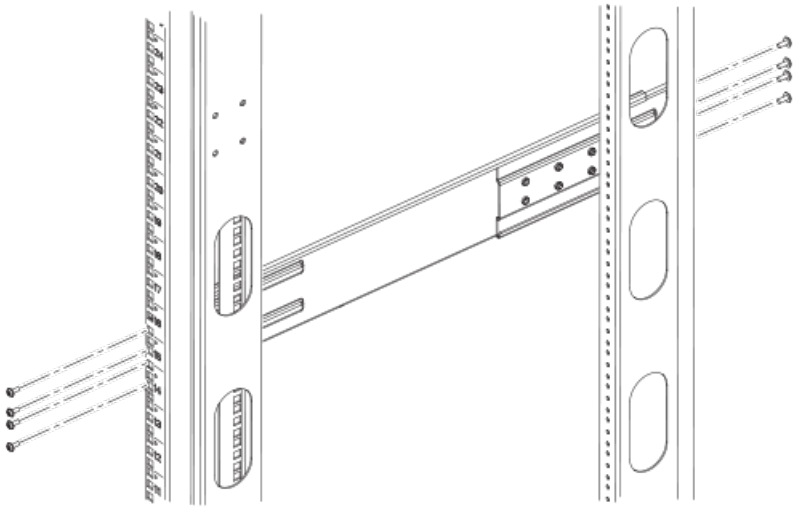
3. Attach the side plates to the router using 8 4-40 flat head screws. Refer to the following figure.

   FIGURE 54 Attach the side plates to the rear sides of the device



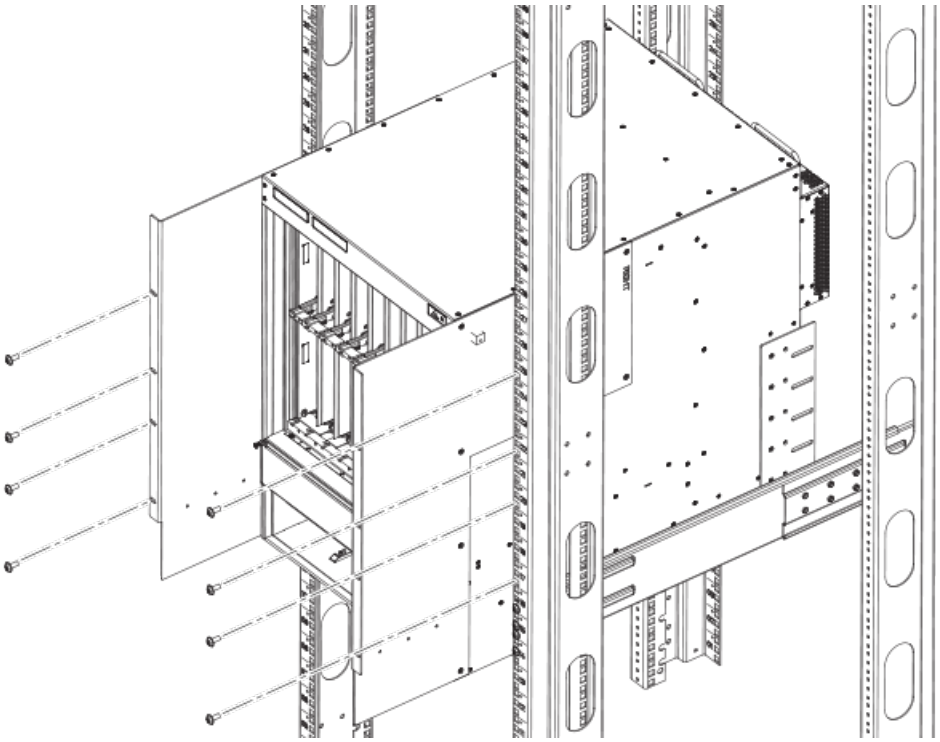
4. Attach the telescoping rails to the mounting posts in the EIA rack. Refer to the following figure.

   FIGURE 55 Attach telescoping rails to EIA rack mounting posts (one rail shown)



5. Install the router in the EIA rack using 8 10-32 screws, as shown in the following figure.

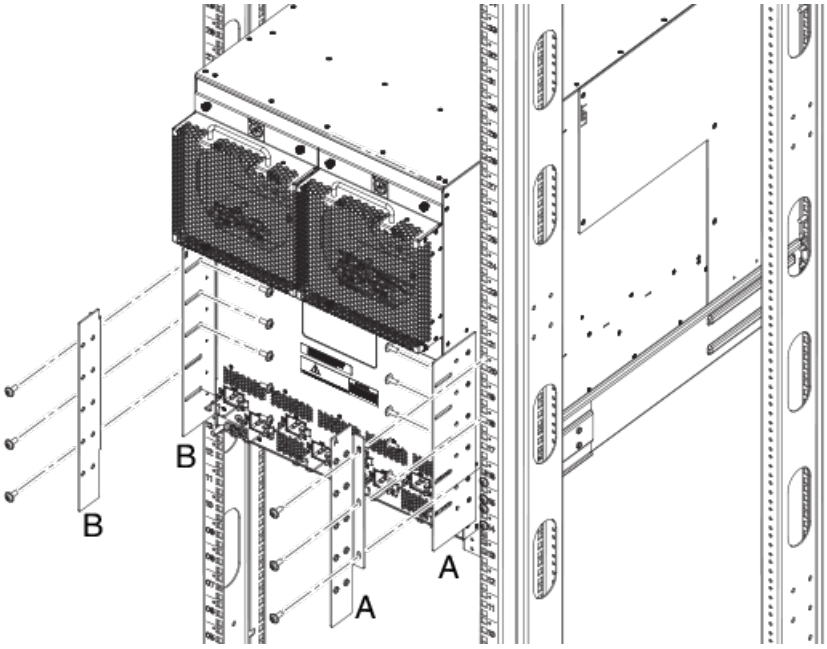
FIGURE 56 Install the router in the EIA rack



6. Secure the transport brackets to the rear of the router using 10 10-32 screws, and to the EIA rack mounting posts using 6 10-32 screws, as shown in the following figure.

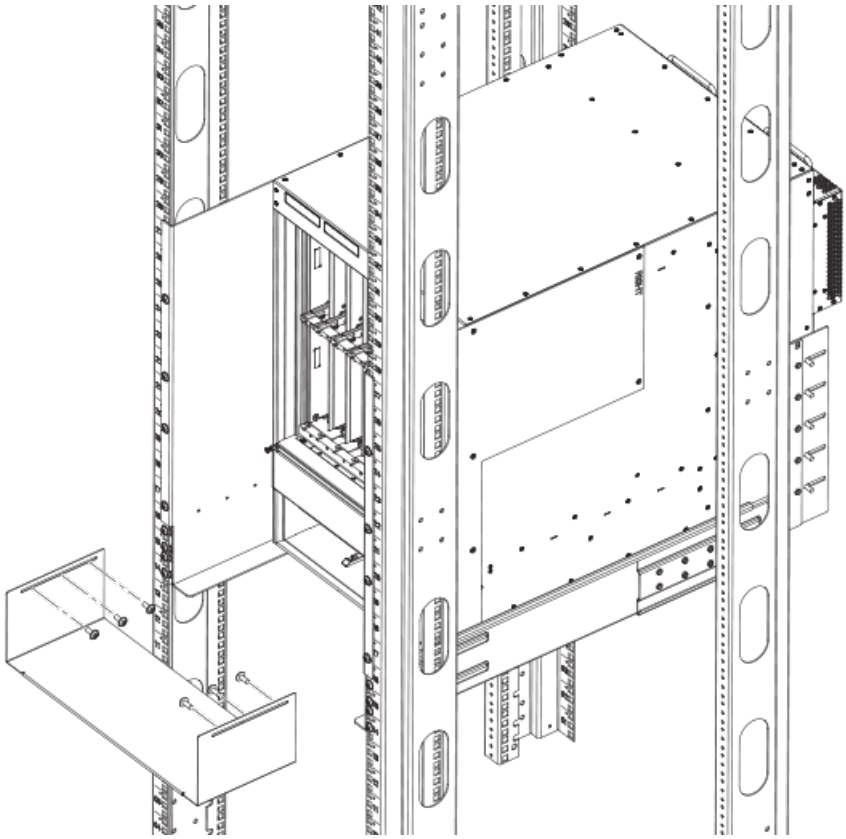
   NOTE
   The transport brackets provide extra stability, and must be installed if you plan to ship the device while it is mounted in the EIA rack. Before you install the transport brackets, you must first remove any installed fans.

FIGURE 57 Secure transport brackets to the device and EIA rack mounting posts



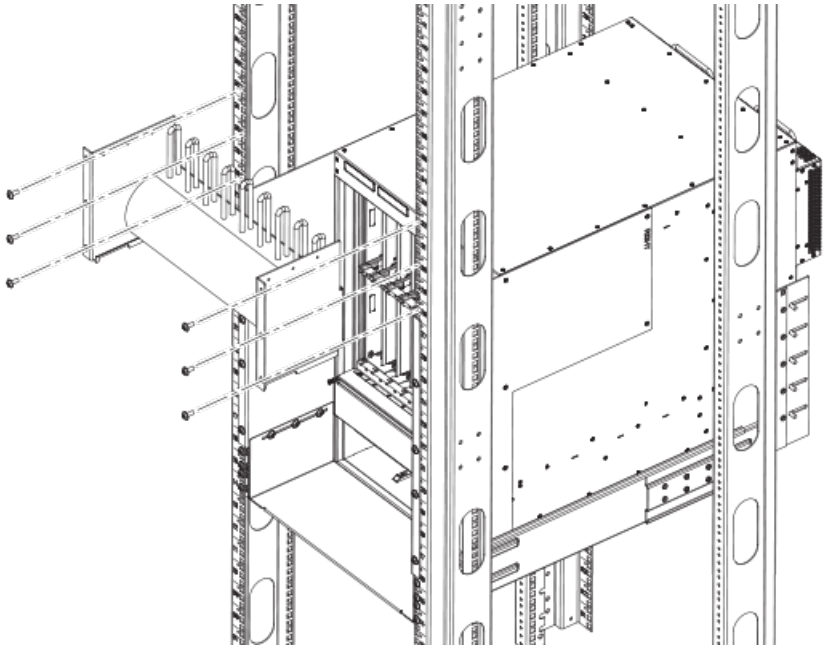
7. Attach the air block bracket to the front of the EIA rack. Refer to the following figure.

FIGURE 58 Install the air block bracket



8. Attach the cable management comb as shown in the following figure. For cable management instructions, refer to MLXe-32 router cable management on page 156.

FIGURE 59 Attach the cable management comb



NOTE
Repeat these steps for each router you install in the EIA rack.

Installing an MLXe-32 router

This section describes how to install an MLXe-32 router.

NOTE
Illustrations in this chapter may differ slightly from the actual equipment.

Preparing the installation site

Before installing the router, plan the location and orientation relative to other devices and equipment. For cooling purposes, allow a minimum of six inches of space between the sides, front, and the back of the router and walls or other obstructions. If a router is installed within a perforated enclosure, the perforations must cover at least 60 percent of the surface.

NOTE
This equipment is suitable for installation in a Network Telecommunication facility and where NEC requirements apply. Additionally, it may be installed in either a Common Bonding Network (CBN) or Isolated Bonding Network (IBN). It is not intended for Outside Plant (OSP) installations.

You will need to use a mechanical lift to move and install the router. Be sure to allow enough working room for the lift.

NOTE
Make sure your site provides 200-240 AC power.

Ensure that the proper power and network cabling is installed at the site.

For information on cabling, refer to MLXe-32 router cable management on page 156, Installing power supplies in an MLXe-32 router on page 166, and Attaching a management station on page 171.

MLXe-32 router shipping carton contents

The MLXe-32 router ships with the following items:

- Router chassis with the empty slots covered with upper and lower shipping panels. The router is housed in a wooden shipping crate that is strapped to a pallet.
- The appropriate number of interface modules, switch fabric modules, management modules, and power supplies (four AC or four DC) in separate shipping cartons.
- 32 slot blanks in separate shipping carton.
- Insertion or extraction tool for use with RJ-45 and fiber-optic connectors.

If any of these items are missing, contact the place of purchase.

Unpacking your MLXe-32 router

You will need the following tools to remove your router from the shipping crate:

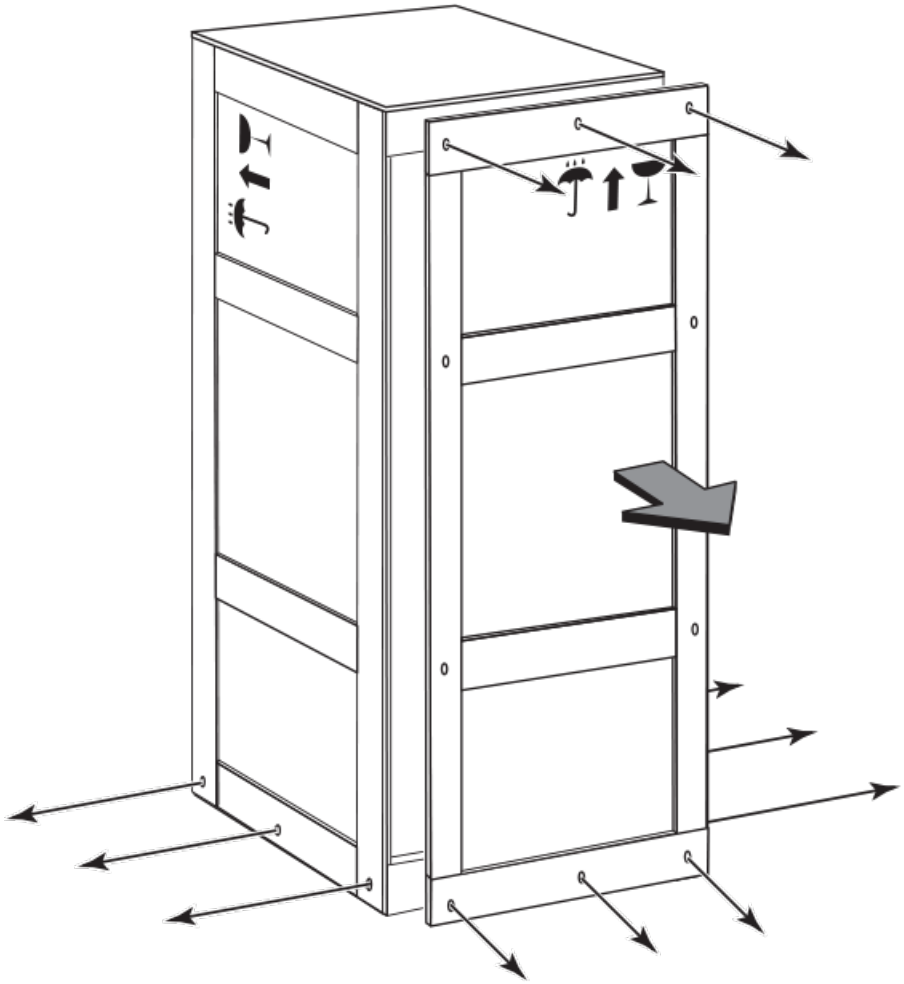
- A forklift or pallet jack with a minimum limit of 550 lbs to move the router crate on the pallet.
- A mechanical lift with a minimum 350 lb limit to move the router off the pallet. The ideal lift configuration is a counterweight base material lift with a metal lift plate installed in place of the forks. The metal plate should be no wider than 17 inches, so that it will fit between the rack mount rails.
- A strap to stabilize the router while you are moving it on the mechanical lift.
- A power drill with the following attachments:
  - Large Phillips screwdriver
  - Large flat-blade screwdriver
  - 7/16-inch socket wrench

The MLXe-32 router ships in a wooden crate bolted to a wooden platform that rests on a pallet. Follow these steps to uncrate the router.

1. The router shipping crate must be in the upright position with enough space to slide the crate off of the pallet.

2. Use a power drill with Phillips and large flat-blade screwdriver attachments to remove the bolts and screws that hold the front shipping crate panel in place, as shown in the following figure. Remove the front panel and set it aside.

   FIGURE 60 Removing bolts and screws and the front panel of the shipping crate



3. Remove the remaining bolts and screws that attach the bottom of the crate to the pallet.
4. Slide the sides, top, and back of the crate backwards as one unit until it clears the pallet.
5. Save the crate (including the shipping panel) in case the router needs to be shipped again.

Installing an MLXe-32 router in an EIA rack

DANGER
Make sure the rack housing the device is adequately secured to prevent it from becoming unstable or falling over.

DANGER
Mount the devices you install in a rack as low as possible. Place the heaviest device at the bottom and progressively place lighter devices above.

Because of the weight of a fully loaded MLXe-32 router, it is recommended that you install the router in a rack before installing any modules and power supplies.

You can install one 32-slot router in a standard 19-inch 2-post or 4-post EIA rack, in either a front-mount position or a mid-mount position. You must provide eight standard #12-24 pan-head screws to secure the router in the rack. You will need a #2 Phillips screwdriver to perform this task.

> NOTE
> Because of the weight of a fully-populated 32-slot chassis, it is not recommended that you install your 32-slot router in a 2-post EIA rack. The preferred installation is in a 4-post EIA rack. Refer to Installing your MLXe-32 outer in a 4-post EIA rack on page 143 for installation instructions.

Installation requirements

Allow 1 to 2 hours to complete this procedure. Your installation site must meet the following requirements to ensure correct installation and operation:

- Provide 35 U of space in a 19 inch rack.
- Verify that the additional weight of the router does not exceed the weight limits for the rack or the floor.
- Ensure that an electrical branch circuit with the following characteristics is available:
  - Required voltage and frequency as indicated in the hardware reference manual.
  - Protection by a circuit breaker in accordance with local electrical codes.
  - Supply circuit, line fusing, and wire size that conform to the electrical rating on the router nameplate.
  - Grounded outlet compatible with the power cord and installed by a licensed electrician.
- Ensure that all equipment installed in the rack is grounded through a reliable branch circuit connection. Do not rely on a secondary connection to a branch circuit, such as a power strip.
- Ensure that the rack is mechanically secured to support the router model.Ensure that the airflow available at the inlet air vents does not exceed 40o Celsius (104o Fahrenheit).
- Only one 32-slot device can be mounted per rack, positioned as close to the bottom of the rack as possible.
- The empty device weighs approximately 362 lbs. You will need a mechanical device (such as a material lift), and at least two people to guide the device into place.
- Before you install the device, make sure that the rack is in a permanent location and is secured to the floor or wall of the building. The installation site must allow adequate clearance for airflow, installation, and maintenance.

Tool requirements and parts list

You will need the following tools to install a 32-slot device in any EIA rack.

- A forklift or pallet jack to move the router while it is on the pallet (500 lbs. minimum).
- Insertion-extraction tool for use with RJ-45 and fiber-optic connectors
- A mechanical lift tool fitted with a lift plate (instead of forks) to move the device off the pallet and transport it to the rack. The lift should be rated for 500 lbs. minimum.
- A strap to secure and stabilize the device while it is being moved on the mechanical lift
- A power drill with the following attachments:
  - Large #2 Phillips screwdriver attachment
  - A 7/16 inch socket wrench attachment
  - Large 3/8 inch flat blade screwdriver attachment

Preparing the installation site

Before installation, plan the location and orientation of the device relative to other equipment in the rack. For cooling purposes, allow a minimum of six inches of space between the front and back of the device, and walls or other obstructions.

Because you will need to use a mechanical lift to move and install the device, make sure you allow enough space to operate the lift. You will also need at least two people to slide the router off the lift and into the rack.

Preliminary EIA rack mount installation steps

Follow these initial steps to mount a 32-slot device in any EIA rack. To install your device in a 2-post EIA rack (not recommended), refer to Installing your MLXe-32 router in a 2-post EIA rack on page 138. To install your device in a 4-post EIA rack, refer to Installing your MLXe-32 outer in a 4-post EIA rack on page 143.

1. Ensure the rack is in a permanent location and is secured to the building. Ensure that the installation site allows adequate clearance for airflow, installation, and maintenance.
2. Move the pallet and router as close to the installation site as possible.
3. Remove the chassis from the shipping pallet.
4. Position the mechanical lift equipped with a lift plate as close to the front of the router as possible. Adjust the lift plate height so that it is even with the bottom of the router.
5. Slide the router onto the lift plate.

   DANGER
   Do not attempt to lift an ExtremeRouting MLX-32 chassis. It is extremely heavy. REMOVE THE POWER SUPPLIES AND INTERFACE MODULES FIRST (management, switch fabric, and all line cards). Use a mechanical lifting device to lift the chassis. Four or more people are required to position the unpopulated chassis into the rack.

   CAUTION
   To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

6. Secure the router to the mechanical lift with a strap to prevent tipping.
7. Carefully position the router in front of the rack where it is to be installed.

   NOTE
   Make sure your site provides 200-240V power.

Installing your MLXe-32 router in a 2-post EIA rack

NOTE
Because of the weight of a fully-populated 32-slot chassis, it is not recommended that you install your 32-slot router in a 2-post EIA rack. The preferred installation is in a 4-post EIA rack. Refer to Installing your MLXe-32 outer in a 4-post EIA rack on page 143 for installation instructions

You can install your 32-slot device in a 2-post EIA rack in either a front-mount configuration or a mid-mount configuration using the factory-installed mounting brackets. For a mid-mount configuration, simply remove the factory-installed mounting brackets from the front edges of the device and re-attach them to the center sides of the device using the pre-drilled holes.

Once you have completed the preliminary installation preparations (refer to Preliminary EIA rack mount installation steps on page 138), complete the following steps to install your router in a 2-post EIA rack.

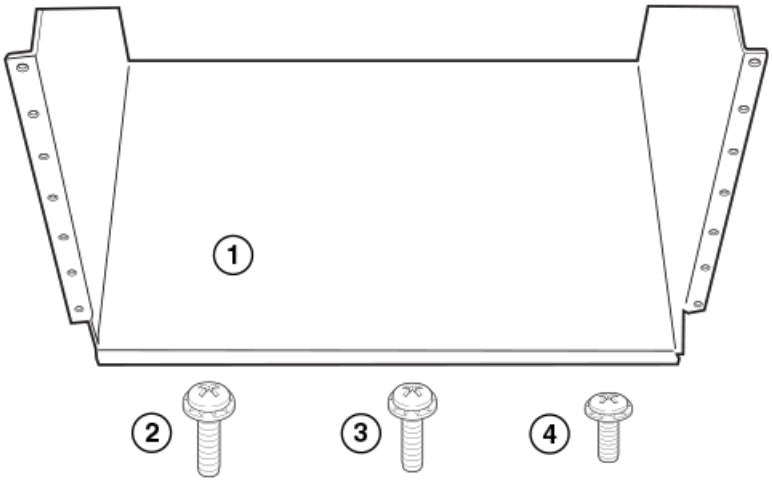
1. Unpack the Open Frame EIA 310-D Rack Mount Kit. The following table provides you with a list of the kit components, and the following figure shows you the contents.

TABLE 32 Open Frame EIA 310-D Rack Mount Kit contents

Part Number	Description	Quantity
42-1000452-01	Saddle	1
52-0000211-01	10-32 x 5/8 inch screws	14
52-1000141-01	12-24 x 1/2 inch screws	14
52-1000138-01	M6 x 12 mm screws	14

NOTE
Use the screws specified for the type of rack. Make sure you have the items listed in the previous table, and shown in the following figure.

FIGURE 61 Open Frame EIA 310-D Rack Mount Kit contents



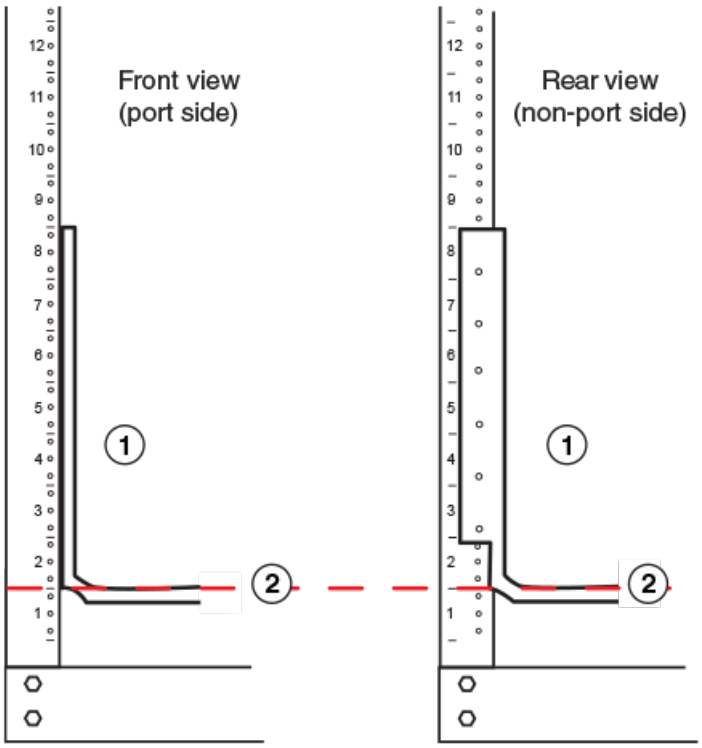
1. Saddle
2. 10-32 x 5/8 inch screws
3. 12-24 x 1/2 inch screws
4. M6 x 12 mm screws

2. Allow 35U in the rack to accommodate the router. Refer to the following figure for system alignment.
   - The saddle requires 1U of permanent space in the rack.
   - The router requires 33U of space in the rack, plus 1U temporary space above for installation.

3. Align the holes in the saddle with the holes on the mounting posts and attach the saddle using a minimum of eight standard pan head screws that were provided in the kit, either #12-24, #10-32, or M6, as appropriated for your rack (four screws on each post, in the three top holes and one bottom hole). See Figure 63.

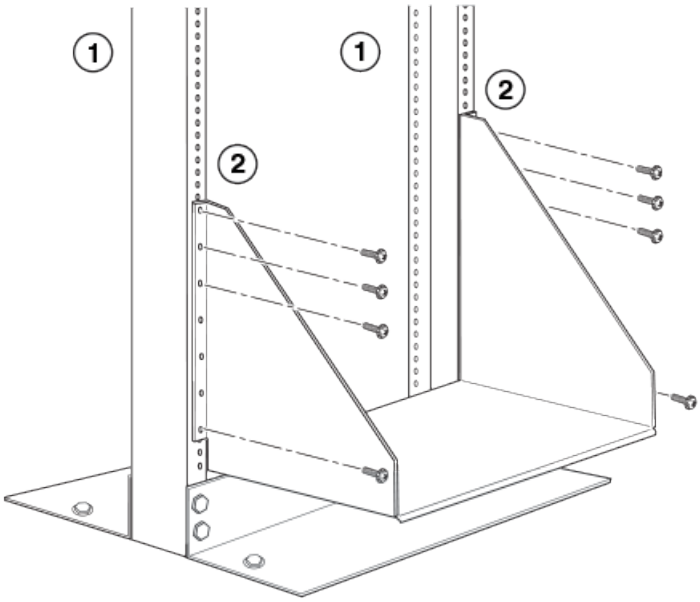
   NOTE
   Additional screws may be used for more support.

FIGURE 62 Align the saddle in the rack



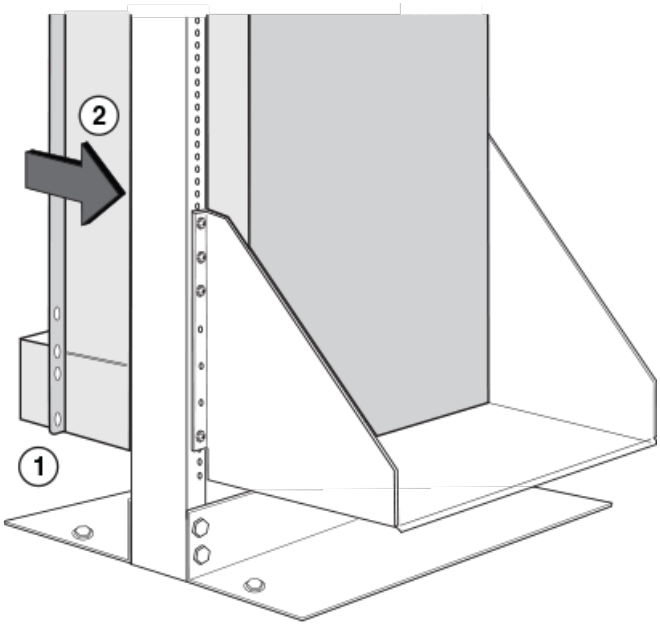
1. Saddle
2. Seat of saddle aligns with U marking on mounting posts as shown

FIGURE 63 Saddle installation



1. Front (port side) of rack mounting post
2. Rear side of rack mounting post

FIGURE 64 Slide the device into the rack

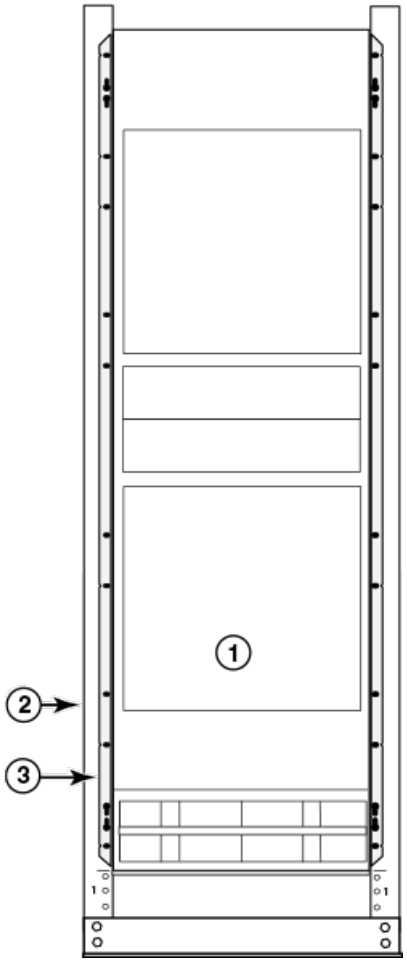


1. Align bottom of router slightly above the seat of the saddle using mechanical lift
2. Using at least two people, slide router gently onto saddle and into the rack

4. Use the provided standard #12-24, #10-32 or M6 pan head screws (dependent on the specifications of your rack) in each available hole on the rack mount bracket to attach the router to the rack mounting poles, as shown in the following figure.

5. Visually inspect the alignment of the router. If the router is installed properly, the mounting screws on both sides rack should be aligned with the mounting screws on the opposite side and the router should be level.

FIGURE 65 Secure the router to the rack



1. Router installed in open frame rack
2. Rack mounting poles
3. Router mounting brackets

6. Remove the strap securing the router to the mechanical lift.
7. With two people in front and two people in back, slide the router into the rack.
8. For a mid-mount, remove the factory-installed mounting brackets from the front edges of the device. Re-attach the mounting brackets to the center sides of the device using the pre-drilled holes in the device. For a front-mount, use the brackets as they were installed at the factory.
9. If you are installing the router in a standard rack, install a mounting screw and a cage nut into each of the holes on the rack posts aligned with the threaded holes in the spacer bars.

NOTE
When connecting the chassis to the rack frame, use thread-forming screws and paint-piercing washers.

10. Visually inspect the alignment of the router. If the router is installed properly in the rack, the mounting screws on one side of the rack should align with the mounting screws on the opposite side and the router should be level. Add all remaining screws.

    NOTE
    For better grounding of the router to the rack, attach the router using star washers. You should also use star washers with any single-hole grounding lugs to keep the lugs from rotating.

Installing your MLXe-32 outer in a 4-post EIA rack

You can install the MLXe-32 routers in a 4-post EIA rack using the optional 4-post rack mount kit available from Extreme Networks. The table below lists the contents of this kit.

TABLE 33 4-Post Rack Mount Kit contents

Part number	Description	Quantity
49-1000166-01	27-31" rail, left	1
49-1000167-01	27-31" rail, right	1
42-1000901-01	Rack mount bracket, left	1
42-1000902-01	Rack mount bracket, right	1
42-0200036-01	Washer, alignment	16
52-0000211-01	Screw, 10-32X.63"	16
52-0200270-01	Nut, floating clip 10-32	16
52-0000210-01	Nut, retainer, 10-32	16
52-1000136-01	Screw, 8-32X.375	10
52-1000138-01	Screw, M6X1.0X12	16

NOTE
Because of the weight of fully loaded 32-slot routers, it is recommended that you mount the router in the EIA rack before installing modules and power supplies.

You will need the following items to install your 32-slot router in a 4-post EIA rack:

- A mechanical lift fitted with a lift plate (instead of forks) to move the device off the pallet and transport it to the rack. The lift should be rated for 500 lbs. minimum.
- A strap to secure and stabilize the device while it is being moved on the mechanical lift.
- Screws to attach the rails to your EIA rack type. (These are usually provided with the EIA rack.)

DANGER
Do not attempt to lift an ExtremeRouting MLX-32 chassis. It is extremely heavy. REMOVE THE POWER SUPPLIES AND INTERFACE MODULES FIRST (management, switch fabric, and all line cards). Use a mechanical lifting device to lift the chassis. Four or more people are required to position the unpopulated chassis into the rack.

CAUTION
To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

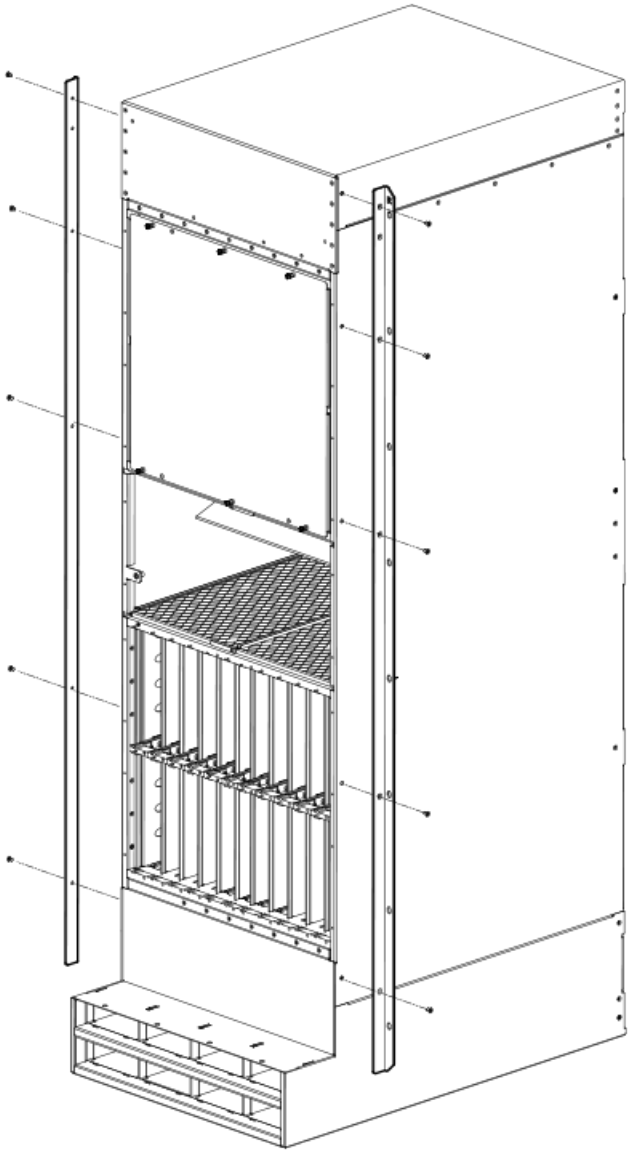
Before installation, plan the location and orientation of the device relative to other equipment in the rack. For cooling purposes, allow a minimum of six inches of space between the front and back of the device, and walls or other obstructions.

Because you will need to use a mechanical lift to move and install the device, make sure you allow enough space to operate the lift. You will also need at least two people to slide the router off the lift and into the rack.

Once you have completed the preliminary installation preparations (refer to Preliminary EIA rack mount installation steps on page 138), follow these steps to mount your 32-slot router in a 4-post EIA rack.

1. Remove the factory-installed mounting brackets from the router chassis.
2. Attach the front right and left mounting brackets to the chassis using 10 8-32 Phillips flat head screws (provided). Refer to the following figure.

FIGURE 66 Attach front right and left mounting brackets to the router chassis

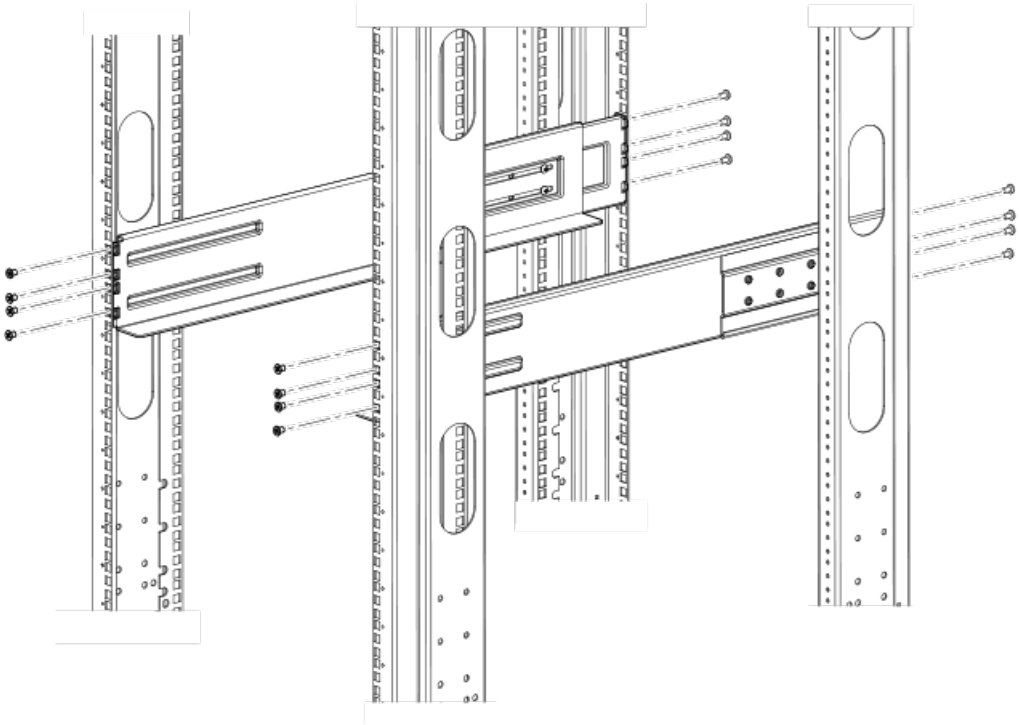


3. Adjust the telescoping rails to fit your rack. The rails can accommodate rack depths from 27 - 31 inches.

4. Attach the side rails to the front and back of the rack, using M6 screws. Refer to the following figure.

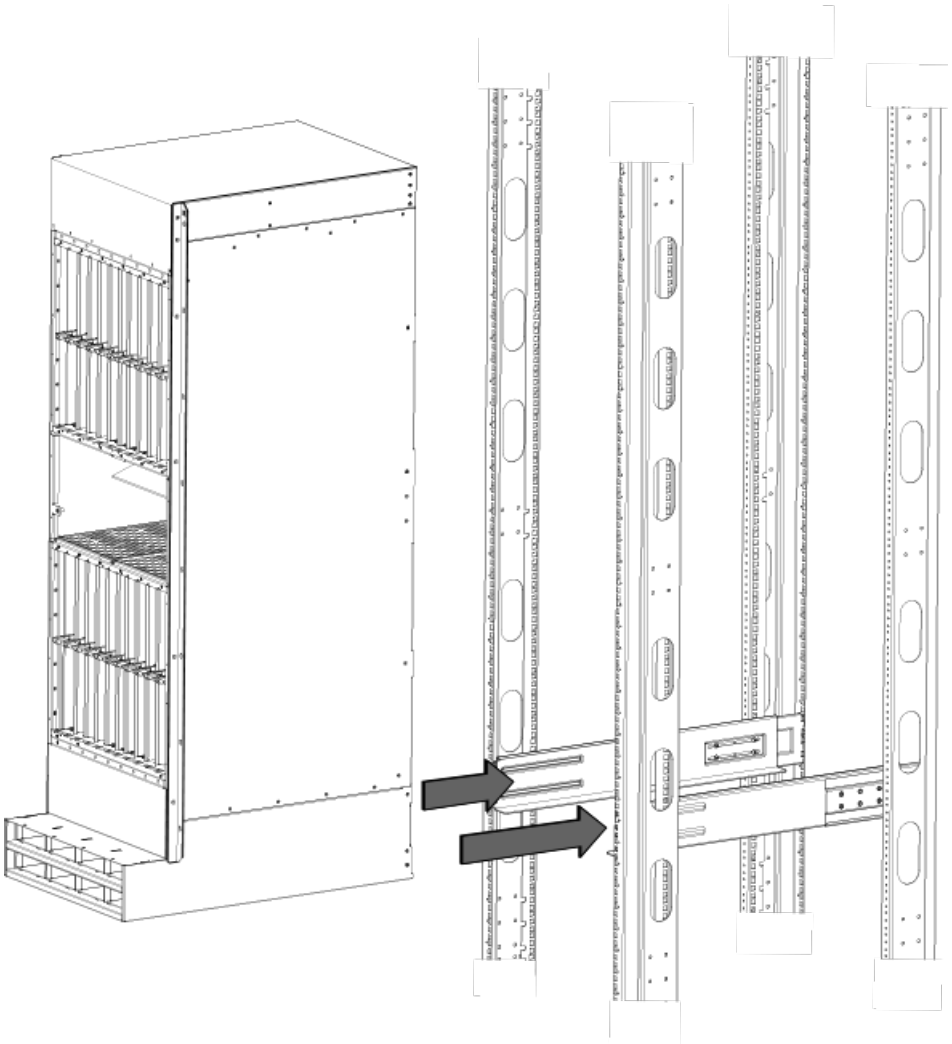
   NOTE
   The narrow telescoping ends of the side rails should attached at the back of the rack.

FIGURE 67 Attach the telescoping side rails to the rack.



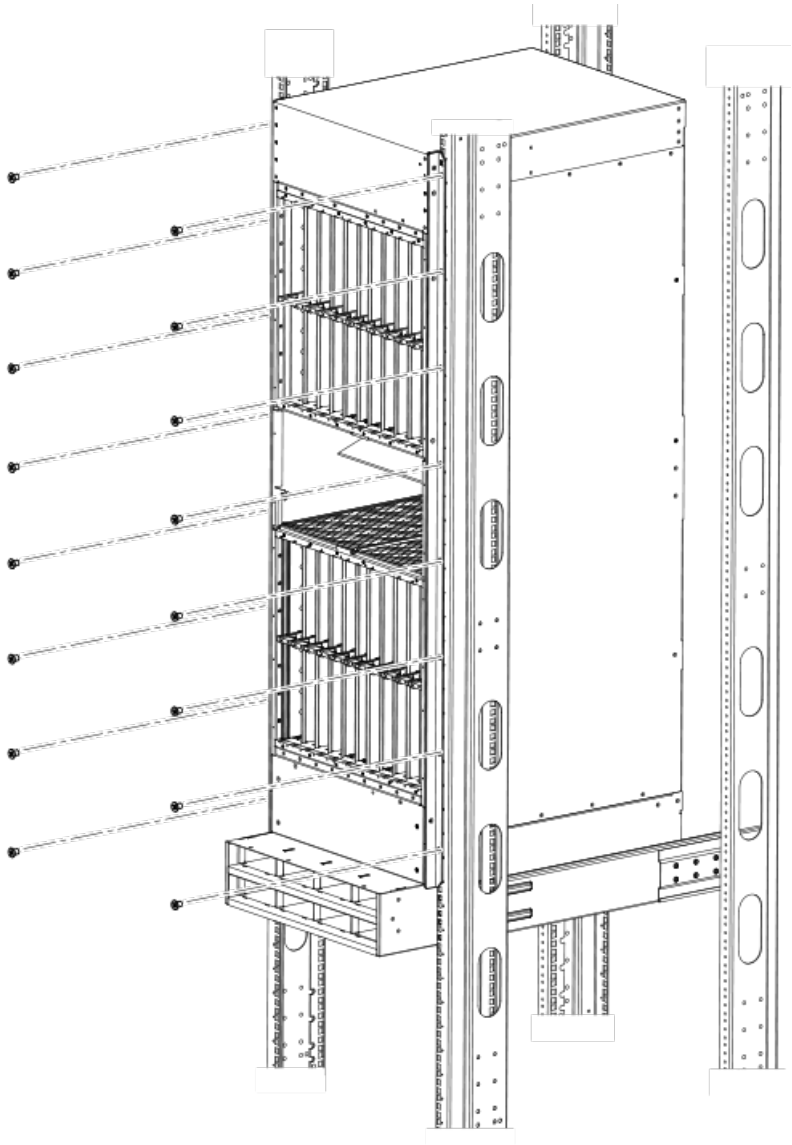
5. Use the mechanical lift to position the chassis as close to the rack as possible. Slide the chassis off the lift and onto the side rails and gently guide the chassis into the rack. Refer to the following figure.

FIGURE 68 Slide the chassis in the rack



6. Once the chassis is securely inserted in the rack, fasten the mounting ears to the front rails of the rack using 10-32x.63 Phillips Square cone screws. Refer to the following figure.

FIGURE 69 Secure chassis in rack



Your rack installation is complete.

Installing the rack mount kit on a 32-slot router in a four-post flush-mount EIA rack

You can mount the MLXe-32 routers in a four-post EIA rack using the optional four-post flush-mount rack-mount kit RMK-4POST-MLXE-32.

> **NOTE**
> The RMK-4POST-MLXE-32 rack-mount kit cannot be used for installing the MLXe-32 routers in an EIA rack with doors. For installing an MLX-32 router in an EIA rack with doors, use the RMK-CAB-MLXE-32 rack mount kit which can be purchased from Extreme Networks.

The contents of this kit are listed in the following table.

TABLE 34 Four-post flush-mount rack-mount kit contents

Part number	Description	Quantity	Notes
49-1000166-XX	27-31" rail, left	1	
49-1000167-XX	27-31" rail, right	1	
42-1000901-XX	Rack mount bracket, left	1	Attaches the rack mount brackets to the chassis.
42-1000902-XX	Rack mount bracket, right	1	Used with 52-1000138-01 (M6 Screws) to mount rails 49-1000166-XX and 49-100167-XX
52-1000278-01	8-32 Phillips flat-head screws, black	10	
42-0200036-XX	Alignment Washer	16	
52-0000211-01	10-32 X .63",Phillips Square Cone Screw	16	Secure the chassis in the EIA rack. Used in combination with either 52-0000210-01 or 52-0200270-01, whichever is appropriate for your rack type.
52-0000210-01	Nut,retainer,10-32	16	
52-1000138-01	M6 X 12MM, Phillips Square Cone Screw	16	Used with part number 52-0000211-01.
52-0200270-01	Floating Clip Nut, 10-32	16	Secures the left and right rails to the EIA rack.
			Used with part 52-0000211-01.

NOTE
Because of the weight of fully loaded routers, it is recommended that you mount the router in an EIA rack before installing modules and power supplies.

You will need the following items to install your 32-slot router in a four-post EIA rack:

- A mechanical lift tool fitted with a lift plate (instead of forks) to move the device off the pallet and transport it to the rack. The lift should be rated for 500 lbs. minimum.
- A strap to secure and stabilize the device while it is being moved on the mechanical lift.
- No. 2 Phillips screwdriver

DANGER
Do not attempt to lift an ExtremeRouting MLX-32 chassis. It is extremely heavy. REMOVE THE POWER SUPPLIES AND INTERFACE MODULES FIRST (management, switch fabric, and all line cards). Use a mechanical lifting device to lift the chassis. Four or more people are required to position the unpopulated chassis into the rack.

CAUTION
To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

Before installation, plan the location and orientation of the device relative to other equipment in the rack. For cooling purposes, allow a minimum of six inches of space between the front and back of the device, and walls or other obstructions.

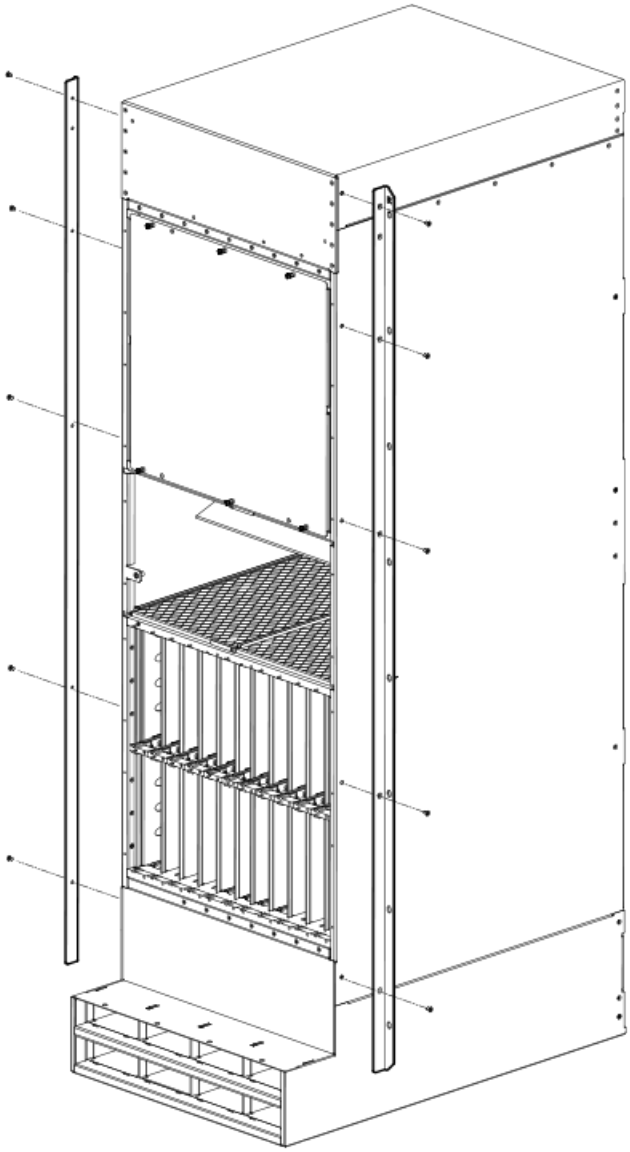
Because you will need to use a mechanical lift to move and install the device, make sure you allow enough space to operate the lift. You will also need at least two people to slide the router off the lift and into the rack.

NOTE

The cable management on this chassis has been removed for clarity to show the installation of the new rack ears and the installation of the device into the rack. The cable management should remain on the chassis during the assembly process.

7. Remove the factory-installed mounting brackets from the router.
8. Attach the front right and left mounting brackets to the chassis using the 10 8-32 Phillips flat-head screws (refer to the following figure).

FIGURE 70 Attaching front right and left mounting brackets to the router chassis

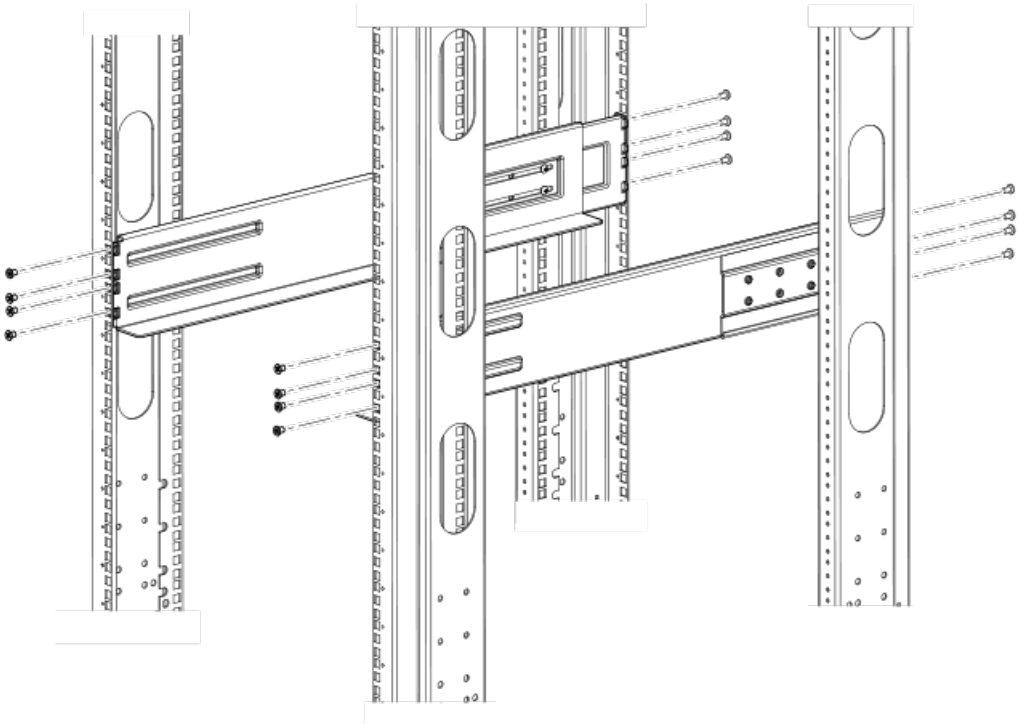


9. Adjust the rails to fit your rack. The rails are telescoping and can accommodate rack depths from 27 through 31 inches.

10. Attach the rails to the front and back of the rack, using screws provided in the kit (refer to the following figure).

    NOTE
    The narrow telescoping ends of the rails should attached at the back of the rack.

FIGURE 71 Attaching the telescoping side rails to the rack.

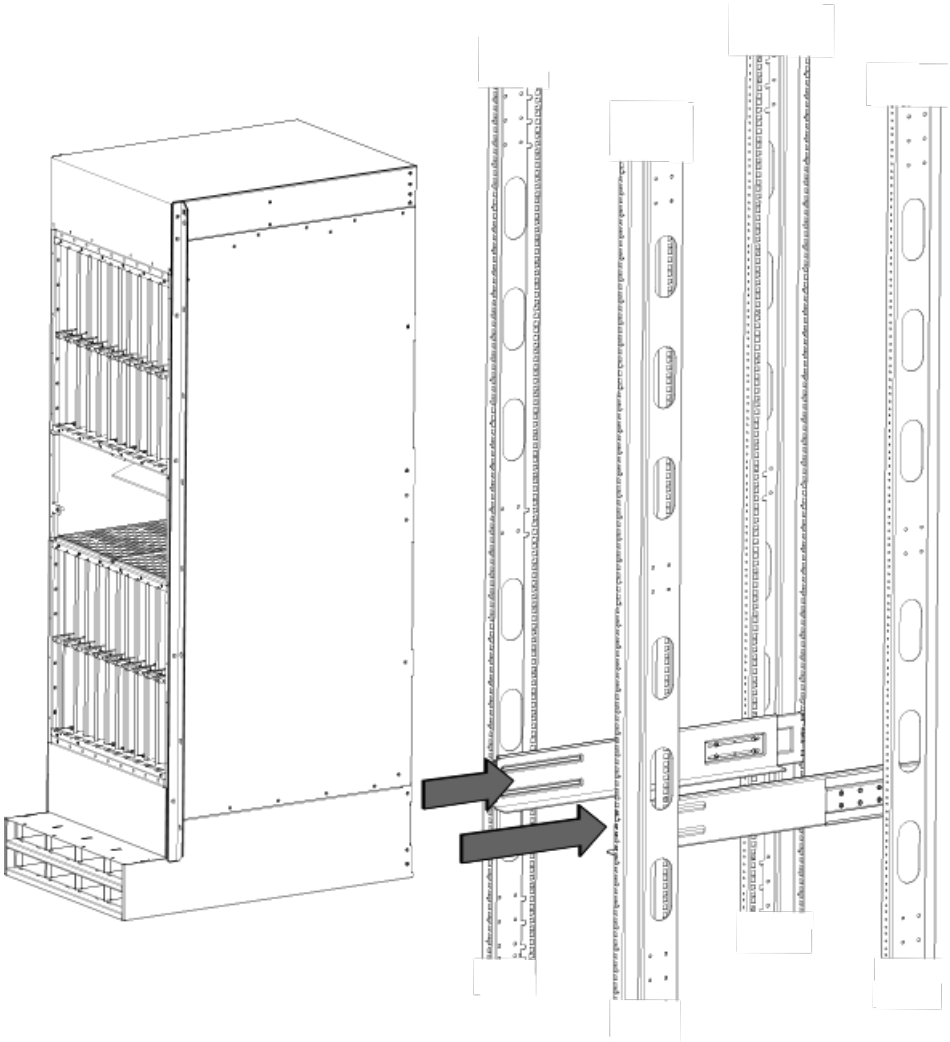


11. Use the mechanical lift to position the chassis as close to the rack as possible. Slide the chassis off the lift and onto the side rails and gently guide the chassis into the rack (see the following figure).

DANGER
Do not attempt to lift an ExtremeRouting MLX-32 chassis. It is extremely heavy. REMOVE THE POWER SUPPLIES AND INTERFACE MODULES FIRST (management, switch fabric, and all line cards). Use a mechanical lifting device to lift the chassis. Four or more people are required to position the unpopulated chassis into the rack.

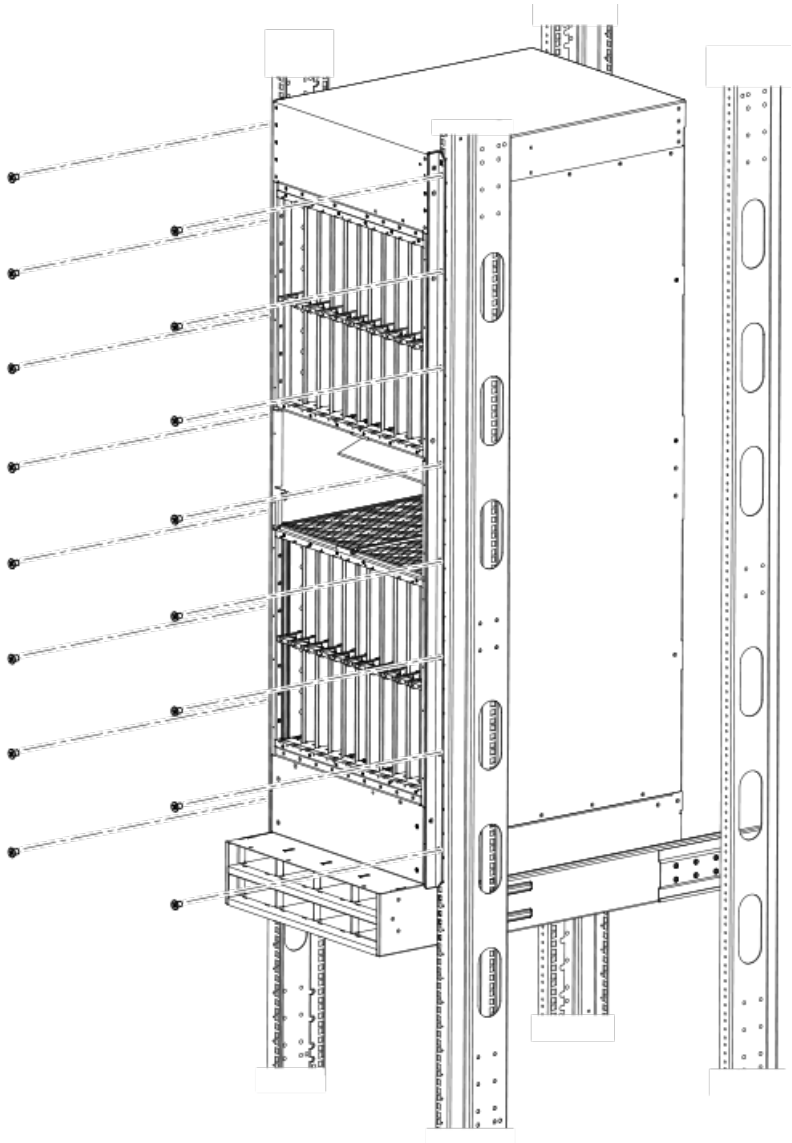
CAUTION
To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

FIGURE 72 Sliding the chassis into the rack



12. Once the chassis is securely inserted in the rack, fasten the mounting brackets to the front rails of the rack using 10-32 screws (eight screws per side) and either clip nuts or floating nuts, whichever is appropriate for your rack type (see the following figure).

    FIGURE 73 Securing the chassis in rack



    Your rack installation is complete.

Installing modules in the MLXe-32 router

The MLXe-32 router ships with empty module slots and upper and lower shipping panels installed.

For instructions about installing 2x100GbE interface modules, refer to Installing 2x100GbE CFP2 interface modules on page 91.

For instructions about installing BR-MLX-10Gx24-DM interface modules, refer to Installing BR-MLX-10Gx24-DM interface modules on page 92.

DANGER
The intra-building port or ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port or ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 5) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

The sequence for installing management, interface, and switch fabric modules is important to ensure proper fit in the MLXe-32 router. When populating the router, start with the middle slot, and work towards the edge. Always fill the bottom slots of the upper and lower card cage of the router first. Refer to MLXe-32 router components on page 26 for slot locations.

During the initial installation of modules, it is recommended that you insert all the modules into the appropriate router slots before tightening the module screws.

For information about how to disable and re-enable power to interface modules, refer to Disabling and re-enabling power to interface modules on page 224.

When populating the 32-slot router, the modules must be installed in the appropriate slots:

- Management modules: management slots 1 and 2
- Switch fabric modules: switch fabric slots 1-8
- Interface modules: Interface slots 1-32

Refer to MLXe-32 router components on page 26 for the locations of these slots.

NOTE
MLX Series router modules are dedicated, which means that you must install them in the MLX Series routers only. If you install an MLX Series module in another Extreme Networks router or a module intended for another Extreme Networks router in the MLX Series router, the router and module will not function properly. Even though management modules are designed to be hot-swappable, you must upgrade the software on all interface modules and management modules to the appropriate software release before installing them. For more information on the appropriate software release, refer to the Hardware Installation Notes that shipped with the management module. If you are installing a redundant management module, refer to the *Extreme NetIron Management Configuration Guide* for information about how the redundant module works, optional software configurations that you can perform, and how to manage the redundancy feature.

Before installing modules in the MLXe-32 router, have the following items available:

- A large flat-head screwdriver.
- An ESD wrist strap with a plug for connection to the ESD connector on the router.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

NOTE
If you are hot-swapping a module, allow a minimum of two seconds after a module (or power supply or fan tray) has been removed before inserting a module in the same slot.

Follow these steps to install a module in the MLX Series router.

1. If you are installing a module into a slot which may have been configured for a different module type, first remove the old configuration information by following these steps:
   a) Use the **show running-config** command in config mode to determine the current configuration of the slot.

      ```
      device(config)# show running-config
      Current configuration:
      !
      ver V5.0.0T163
      module 1 ni-mlx-20-port-1g-copper
      !
      ```

      This example shows that slot 1 has already been configured for a 20-port 1 Gbps copper interface module.

   b) Enter the **no module***slotmodule* command to remove the configuration from slot 1. Use the slot and module information shown as a result of the **show running-config** command.

      ```
      device(config)# no module 1 ni-mlx-20-port-1g-copper
      ```

      The command removes the configuration from slot 1, leaving it ready for a new module.
2. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the chassis.
3. Remove the module from the packaging.
4. Insert the module into the slot, and slide it along the card guide until the ejectors on either side of the module rotate towards the module faceplate, as shown in the following figure.

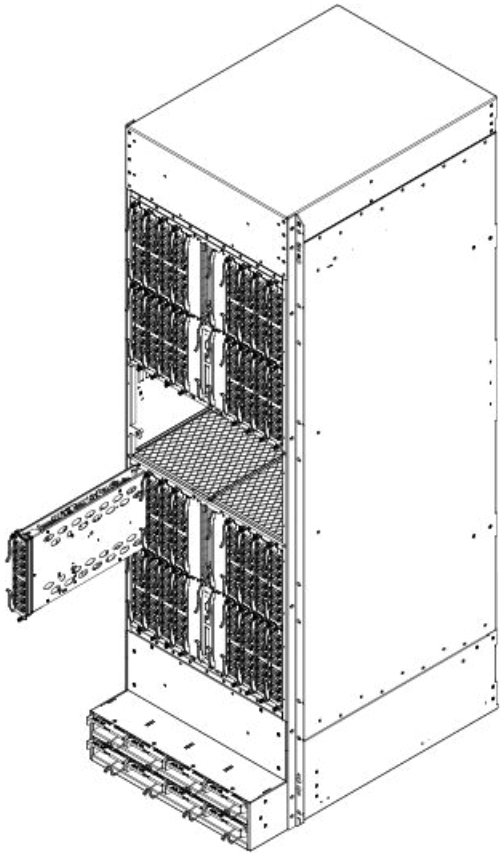
   NOTE
   When inserting the module into the router, make sure that the faceplate doesn't overlap the faceplate of an adjacent module.

5. Rotate the ejectors until they are flush with the module faceplate. This action will fully seat the module in the backplane.
6. Tighten the screws at each end of the module faceplate by pushing them in and turning them clockwise. Complete the tightening process using the flat-blade screwdriver.

7. Enter the **write memory** command to ensure that the slot will be correctly configured for the new module after a reboot.

```
device(config)# write memory
Write startup-config done.
```

FIGURE 74 Installing a module in an MLXe-32 router



Power supply requirements for NI-MLX-1Gx48-T-A modules

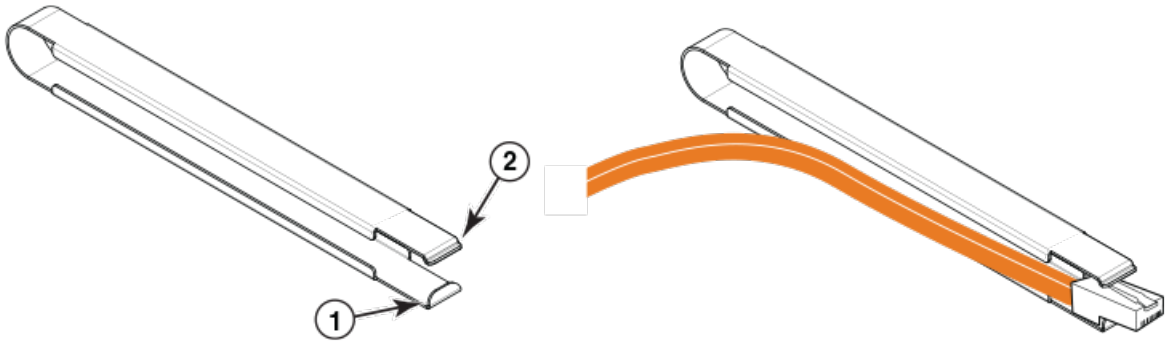
You can install up to twenty NI-MLX-1Gx48-T-A modules and populate the remaining slots with other modules, which requires four 2400W power supplies. You can achieve 4+4 power redundancy by installing four additional power supplies.

If you install 21 or more NI-MLX-1Gx48-T-A modules in your router, you will need a minimum of five power supplies. You can achieve 5+3 power redundancy by installing three additional power supplies.

Using the insertion and extraction tool

Due to the high density of cables that the MLXe-32 router can support, it may be difficult to insert and remove the RJ-45 and optical connectors. An insertion and extraction tool has been provided in the MLXe-32 router accessory kit to make this task easier. The following figure shows this tool and how it is used.

FIGURE 75 insertion and extraction tool



1. Hooked tab
2. Stepped tab

Use the tool to grasp the plug of the modular connector at its narrow end (the end closest to the attached cable), and insert the connector into the proper interface module. Grasping the plug at the wide end during insertion may result in the tool being difficult to release and remove.

When using the tool to extract the plug of a modular connector, cover the entire length of the plug with the tool. Notice that one end of the tool has a "hook" side. Use this side to compress the locking tab while you remove the connector.

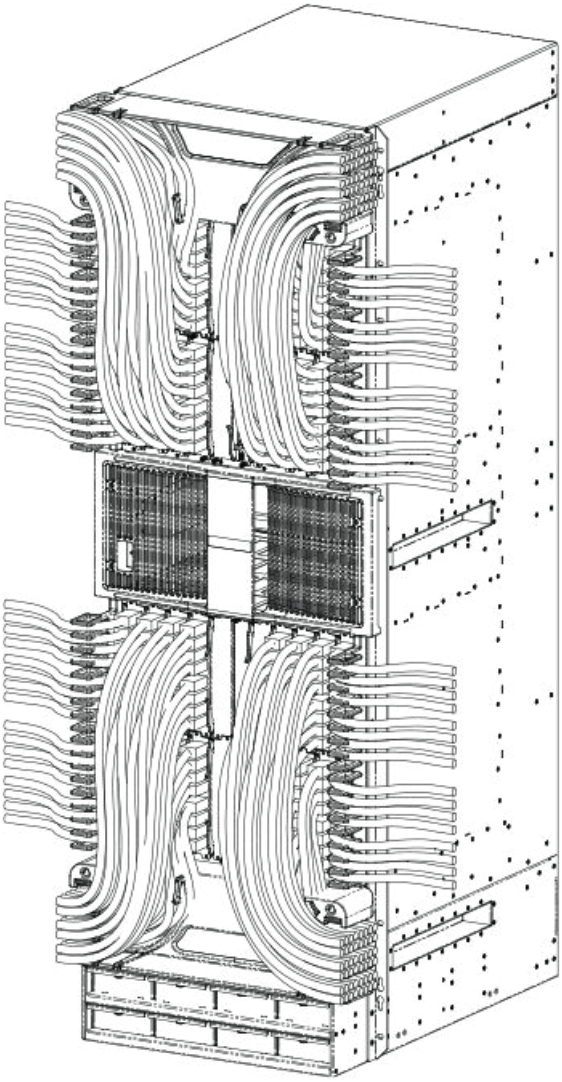
MLXe-32 router cable management

The MLXe-32 router cable management system allows access to the power supplies at the bottom of the router, and keeps the air inlet clear in the center of the router (this is essential for proper cooling). Cable management hardware at the top, bottom and sides of the router make it easier to route the cables in the proper directions.

In general, cables from the outer interface modules are routed horizontally and away from the router. Cables from the remaining modules in the upper half of the router are routed up, then outwards along the channels.

Cables for modules in the lower half of the router follow a similar path downwards, above the power supplies. The following figure shows the cable routing, with the upper and lower cable management system covers removed for clarity. The following sections describe cable routing for each quadrant of the router.

FIGURE 76 MLXe-32 router cable routing diagram



CAUTION
Be sure not to exceed the minimum recommended bend radius for the cables: 2" for MRJ-21 cables, and 1.5" for Category 5 (RJ-45) and fiber-optic cables.

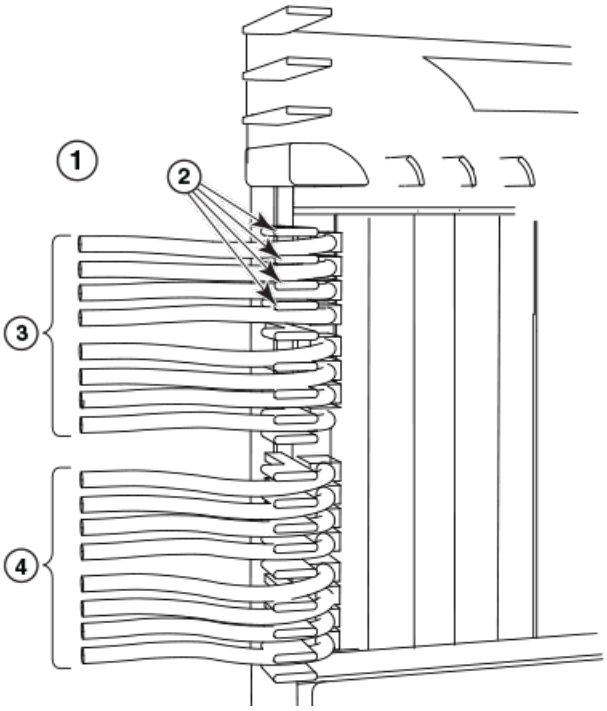
CAUTION
Before plugging a cable into any port, be sure to discharge the voltage stored on the cable by touching the electrical contacts to ground surface.

Cable routing for the upper-left quadrant

Route cabling from slots in numerical order starting with the cables for slot #1.

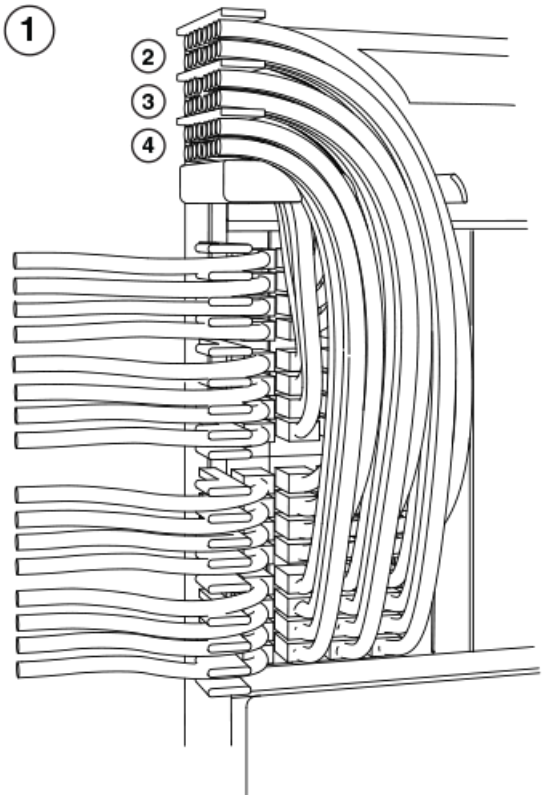
1. Route cables for slots #1 and #2 directly to the left through the side comb, as shown in the following figure.

FIGURE 77 Routing upper-left quadrant cables



1. Upper left quadrant
2. Cables from slot #1
3. Side combs (18)
4. Cables from slot #2

FIGURE 78 Routing upper-left quadrant cables up



1. Upper left quadrant
2. Comb B (slot #5 and #6 cables)
3. Comb C (slot #7 and #8 cables)
4. Comb A (slot #3 and #4 cables)

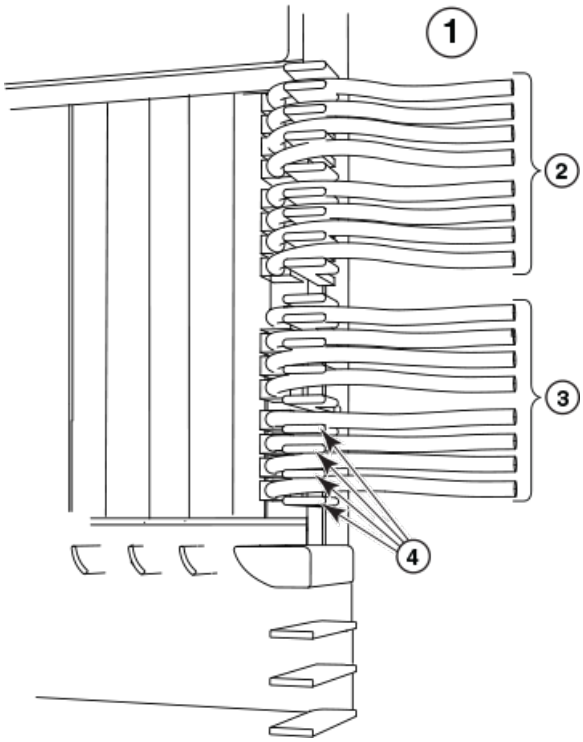
2. Route cables from slots #3 and #4 up through comb A, as showin in the previous figure.
3. Route cables from slots #5 and #6 up through comb B.
4. Route cables from slots #7 and #8 up through comb C.

Cable routing for the upper-right quadrant

Route cables from slots in numerical order starting with the cables for slot #15.

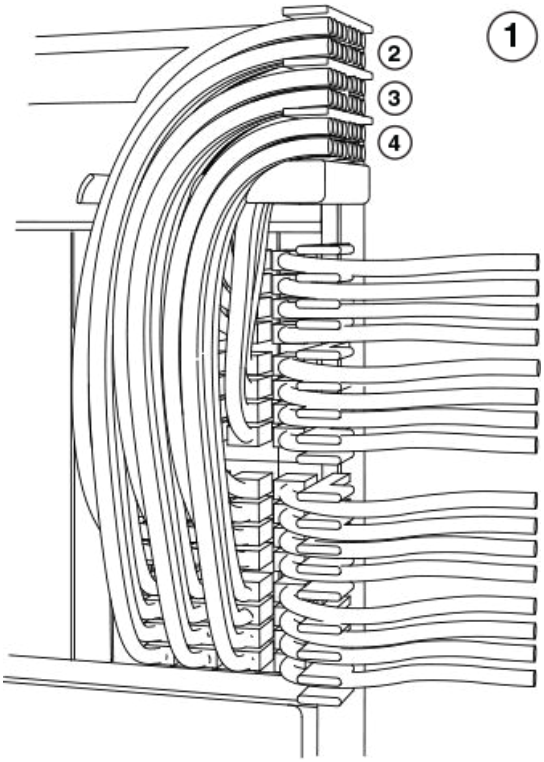
1. Route cables from slots #15 and #16 directly to the right through the side comb, as shown in the following figure.

   FIGURE 79 Routing Upper-right quadrant cables to the right



1. Upper right quadrant
2. Cables from slot #15
3. Side combs (18)
4. Cables from slot #16

FIGURE 80 Routing upper-right quadrant cables up



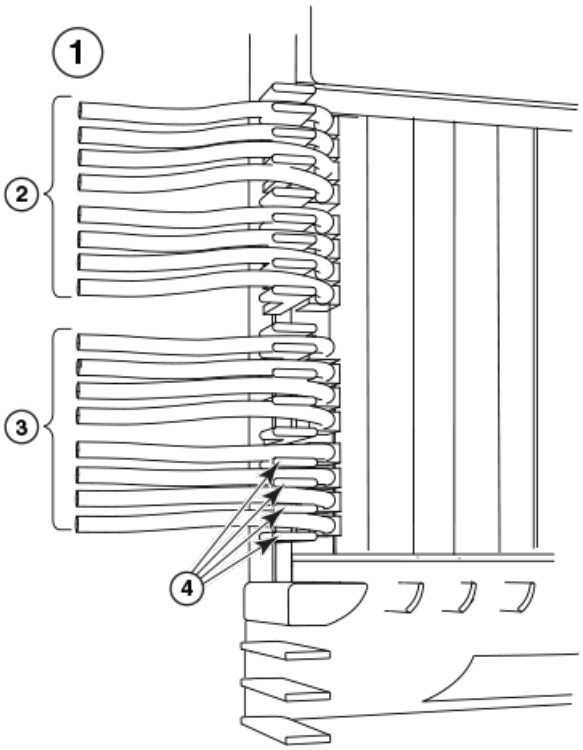
1. Upper right quadrant
2. Comb B (slot #11 and #12 cables)
3. Comb C (slot #9 and #10 cables)
4. Comb A (slot #13 and #14 cables)

2. Route cables from slots #13 and #14 up through comb A, as shown in the previous figure.
3. Route cables from slots #11 and #12 up through comb B.
4. Route cables from slots #9 and #10 up through comb C.

Cable routing for the lower-left quadrant

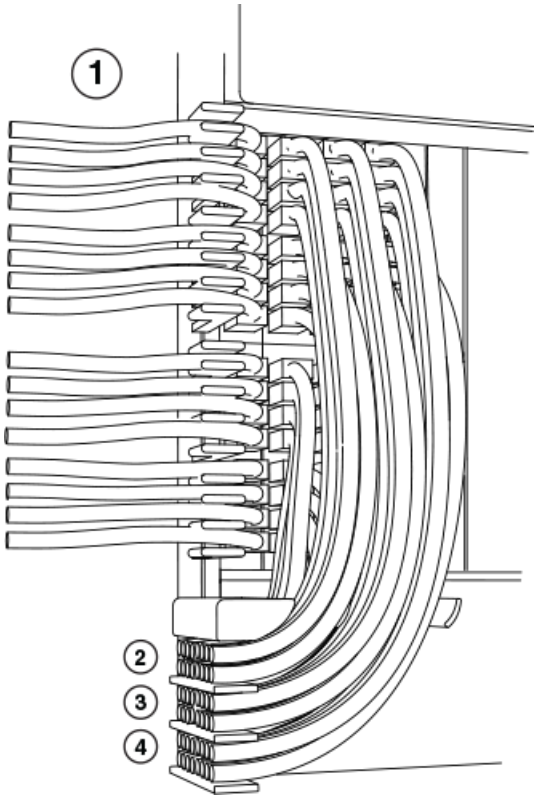
1. Route cables from slots #18 and #17 directly to the left through the side comb, as shown in the following figure.

FIGURE 81 Routing lower-left quadrant cables



1. Lower left quadrant
2. Cables from slot #18
3. Cables from slot #17
4. Side combs (18)

FIGURE 82 Routing lower-left quadrant cables



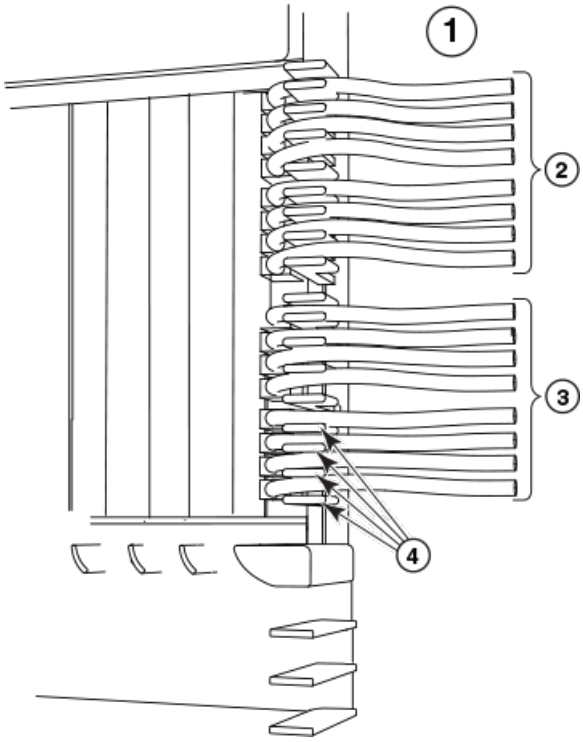
1. Lower left quadrant
2. Comb B (slot #21 and #22 cables)
3. Comb A (slot #19 and #20 cables)
4. Comb C (slot #23 and #24 cables)

2. Route cables from slots #20 and #19 down through comb A, as shown in the previous figure.
3. Route cables from slots #22 and #21 down through comb B.
4. Route cables from slots #24 and #23 down through comb C.

Cable routing for the lower-right quadrant

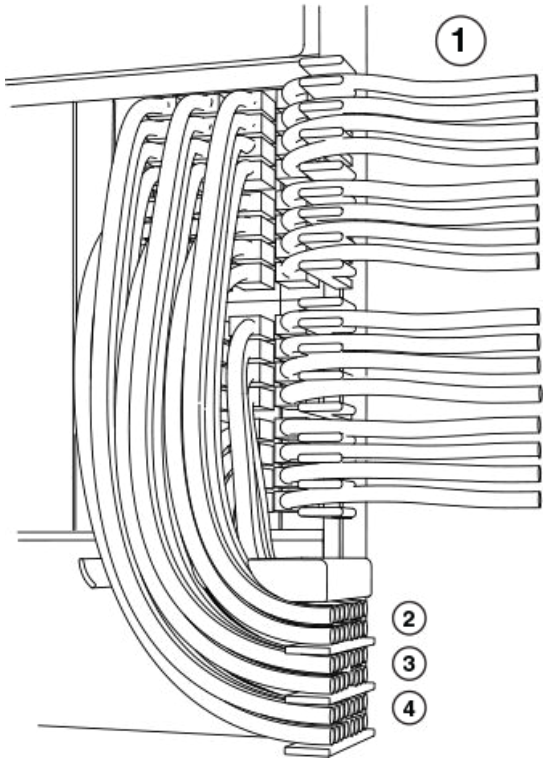
1. Route cables from slots #32 and #31 directly to the right through the side comb, as shown in the following figure.

FIGURE 83 Routing the lower-right quadrant cables



1. Lower right quadrant
2. Cables from slot #32
3. Cables from slot #31
4. Side combs (18)

FIGURE 84 Routing lower-right quadrant cables



1. Lower right quadrant
2. Comb B (slot #27 and #28 cables)
3. Comb A (slot #29 and #30 cables)
4. Comb C (slot #25 and #26 cables)

2. Route cables from slots #30 and #29 down through comb A, as shown in the previous figure.
3. Route cables from slots #28 and #27 down through comb B.
4. Route cables from slots #26 and #25 down through comb C.

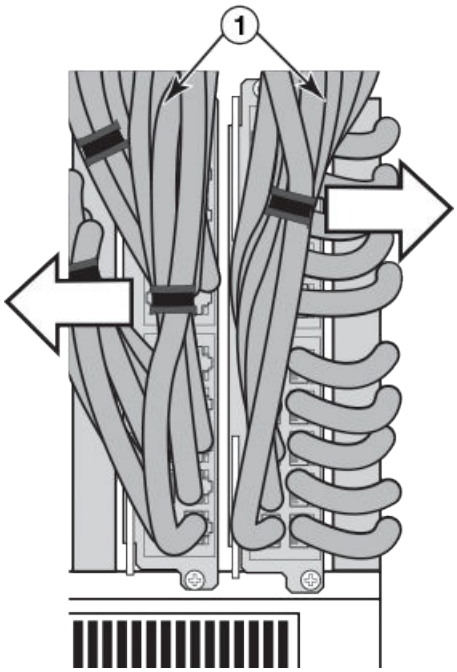
Accessing modules for service

With the cables bundled correctly, it is easier to access the modules for service. Gently move the cable bundles to the side to access a module. Use the appropriate Phillips or flat-blade screwdriver with an extended shaft to disconnect the cables from the module and remove the module. There is no need to undo the cable cinches or cable ties. Refer to the following figure.

NOTE
This procedure is easier with two people. One person can hold the cable bundles aside while the other person loosens the connectors and removes the module.

NOTE
Be careful not to overtighten or cross-thread cable connector screws.

FIGURE 85 Accessing modules by shifting cable bundles



1. Cable bundles

Cable management notes

The following rules apply when setting up cable management for a heavily- or fully-loaded system:

- All cables must be firmly connected, supported, and contained.
- Use cable cinches, spaced approximately every 24 inches, to secure all of the cables for each module into a single bundle. This is especially important at the ends nearest the module connections. Each cable cinch holds up to 8 MRJ21 cables, or 48 RJ-45 cables.
- For additional security, use cable ties to secure cables to the cable management system hardware on the sides of the unit.
- The cable routing slots at the top and bottom of the unit are strong enough to hold many cables, but the more cable cinches and cable ties you use, the more secure your cable management system will be.
- If you bundle the cables correctly, you will be able to move the bundles to the side to access the modules for service, without disturbing the connections. Refer to Accessing modules for service on page 165.
- Always route the cables for the outer-most modules out the sides of the unit. Route the cables for the innermost modules through the top or through the bottom cable management hardware on the unit.

Installing power supplies in an MLXe-32 router

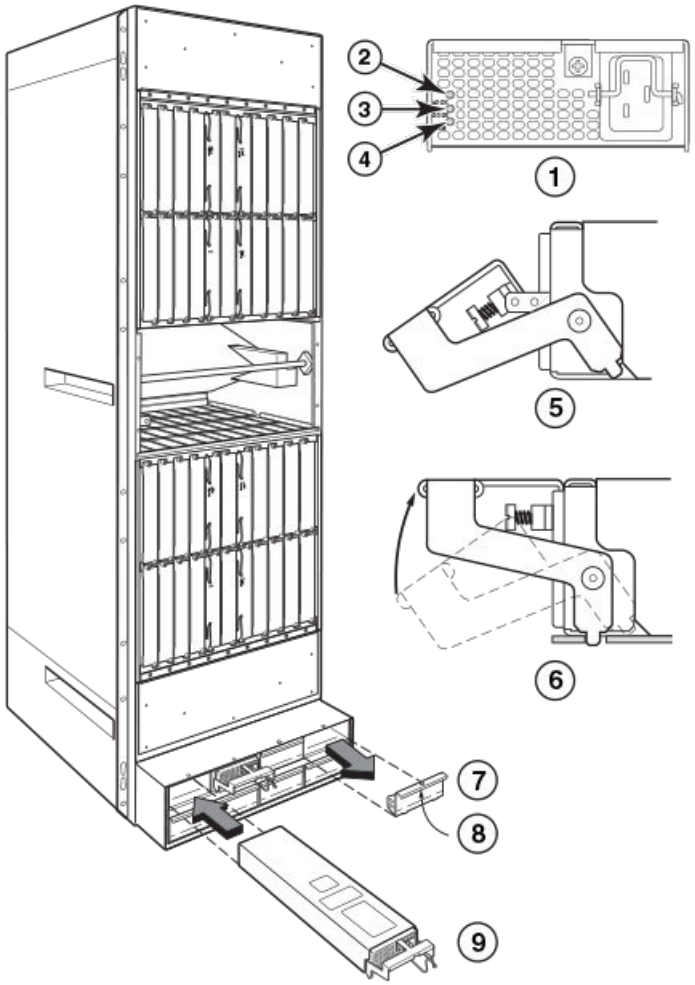
DANGER
High Touch Current. Earth connection essential before connecting supply.

Follow these steps to install a power supply in an MLXe-32 router.

1. Remove the blank power supply faceplate.

2. Remove the power supply from the packaging.
3. Insert the power supply into the slot, using the guides on each side of the slot, as shown in the following figure.

FIGURE 86 Installing a power supply in an MLXe-32 router



1. Power supply indicators
2. AC power input LED (AC OK)
3. DC power output LED (DC OK)
4. Alarm LED (ALM)
5. Latch handle open
6. Lift up latch handle to lock
7. Power supply blank cover
8. Power supply blank cover
9. Power supply

CAUTION
Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

4. Push the power supply front panel toward the back of the router to engage the backplane connector.
5. Pull the release latch on the power supply front panel up to lock the power supply in place.
6. Use a #2 Phillips to screw the locking screw into place.

7. Install a blank power supply faceplate into each empty slot.

   For information about connecting power to the router, refer to Connecting AC power on page 168.

   For information about powering on the system, refer to Activating the power source on page 172.

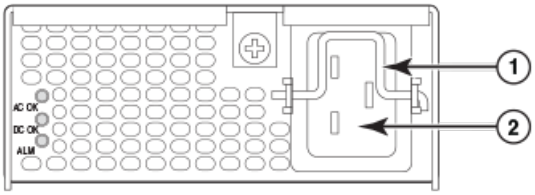
Connecting AC power

NOTE
For the NEBS-compliant installation, AC power connections must use a surge protection device (SPD) to protect the AC power supplies from damage due to excessive power line surges.

AC power is supplied through a power cord that is connected to each power supply in the MLXe-32 router. Follow the steps below to connect AC power to an MLXe-32 router:

1. Locate the power receptacle on each installed power supply, as shown in the following figure.
2. Lift the cord retainer and connect an AC power cord to the power supply.
3. Snap the cord retainer over the power plug to hold it in place.

FIGURE 87 MLXe-32 power supply receptacle and cord retainer



1. Cord retainer
2. Power receptacle

Connecting DC power

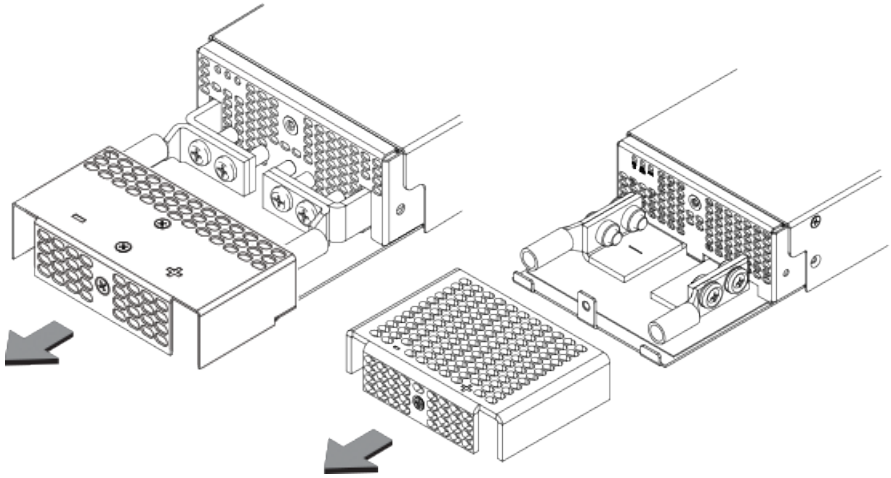
You can use a DC power source for the MLXe-32 router by installing a DC-to-DC power supply. For 2400W power supplies, DC power must be supplied at 48 V and 60 A. For 3000W power supplies, power must be supplied at 48 V and 90 A. The 2400W DC-to-DC supply provides the DC power to the router at 12 V and 200 A. The 3000W DC-to-DC power supply provides the DC power to the router at 12 V and 245 A.

DANGER
The procedures in this manual are for qualified service personnel.

Follow these steps to connect a DC power source.

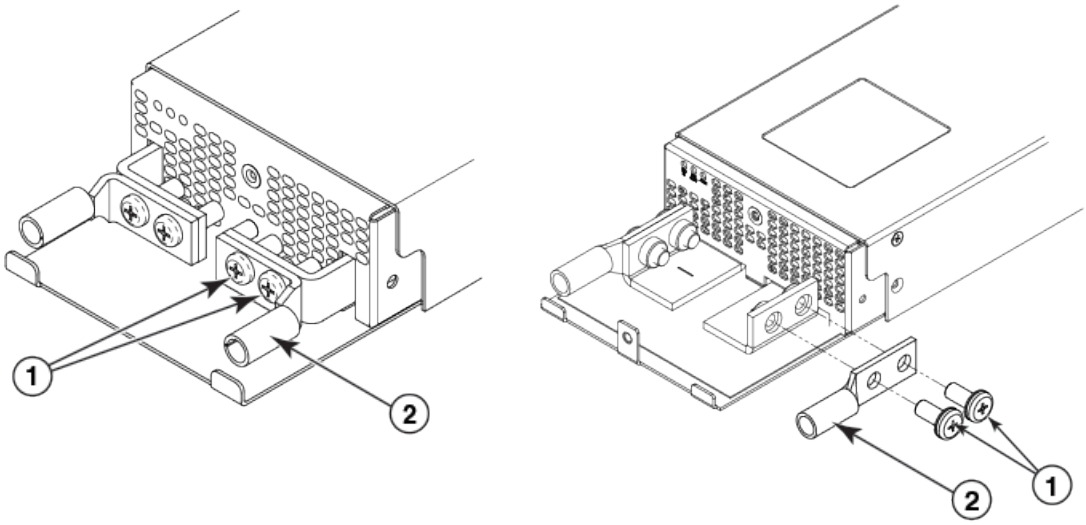
1. Use a #1 Phillips screwdriver to remove the screw that secures the safety cover, as shown in the following figure. Remove the safety cover.

   FIGURE 88 Removing the safety cover (2400W power supply and 3000W power supply displayed)



2. Use a #2 Phillips screwdriver to unscrew the power lugs. Refer to the following figure.

   FIGURE 89 Removing the power lugs (2400W power supply and 3000W power supply displayed)



1. Power lug screws
2. Power lug

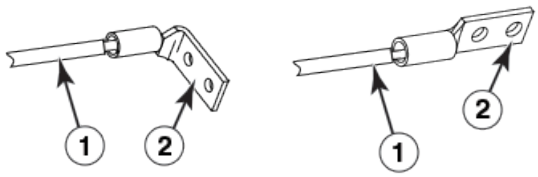
3. Crimp the correct AWG power supply wire into the power lugs. For 2400W power supplies: #4 AWG power supply wire. For 3000W power supplies: #2 AWG power supply wire. Refer to the following figure.

   CAUTION
   For an ExtremeRouting MLX-32 AC system, use a ground wire of at least 2 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

   CAUTION
   For an ExtremeRouting MLX-32 DC system, use a grounding wire of at least 2 American Wire Gauge (AWG). The 2 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. Grounding position is located on the side of the chassis adjacent ground symbol.

   NOTE
   To ensure adequate bonding when attaching the ground lug, a minimum of 20 PSI of torque is required to be applied to the mounting hardware used to attach the ground lug.

   FIGURE 90 Crimping the power supply wire in the lug



1. AWG power supply wire: for 2400W power supply, use #4 AWG; for 3000W power supply, use #2 AWG
2. Power lug

4. Reconnect the power lugs to the power supply unit.
5. Connect the -48V wire to the negative terminal and the 0V wire to the positive terminal.

   NOTE
   DC return must be isolated from the router ground (DC-I) when making connections to the connections to the power supply.

6. Replace the safety cover. Refer to Figure 88.

   This equipment installation must meet NEC/CEC code requirements. Consult local authorities for regulations.

Removing the MLXe-32 router DC power supplies

Follow these steps to remove a 2400W DC power supply in an MLXe-32 router:

1. Ensure the main DC power breaker is OFF.
2. Use a #1 Phillips screwdriver to remove screw that secures the safety cover, as shown in Connecting DC power on page 168. Remove the safety cover.
3. Use a #2 Phillips screwdriver to remove the screws securing the power lugs. Refer to Connecting DC power on page 168.
4. Pull down on handle to remove power supply. Refer to Installing power supplies in an MLXe-32 router on page 166.

   Follow these steps to remove a 3000W DC power supply in an MLXe-32 router:

Final steps

Complete these steps in the order in which they are listed:

- Perform the step Attaching a management station on page 171.
- Perform the step Activating the power source on page 172.
- Perform the step Verifying proper operation on page 172.

Attaching a management station

You can manage your MLX Series router in the following ways:

- Connect a PC or terminal to the console port on the management module. From this port, you can assign an IP address to the management module and establish connections through Telnet or SSH.
- Connect the router to your existing management network and manage the router and other network devices from a management station.

  NOTE
  The management network that you connect to through the 10/100 Ethernet port must be separate and isolated from the network over which user packets are switched and routed. For information about functionality on the management port, refer to Understanding management port functions on page 196.

Attaching a PC or terminal to the console port or Ethernet port

You can attach a PC or terminal to either the console port (which has a male DB-9 serial connector), or the 10/100/1000 or 1000Base TX Ethernet port (which has an RJ-45 UTP connector) on the management module. From the console port, you can access the router CLI directly from the PC or terminal or through a Telnet connection. From the Ethernet port, you can access the router CLI or Web management interface directly from the PC or terminal or through a Telnet connection.

Before performing this task, have the following items available.

- PC running a terminal emulation application or a terminal.
- For console port connections, a straight-through EIA or TIA DB-9 serial cable with one end terminated in a female DB-9 connector and the other end terminated in a male or female DB-9 or DB-25 connector, depending on the specifications of your PC or terminal. You can order this cable from Extreme or build your own cable. If you build your own cable, refer to the pinout information in Console port pin assignments on page 275.
- For Ethernet port connections, a Category 5 UTP crossover cable, which you must supply. For information about the management port pin assignments, refer to Management port pin assignments on page 276.

Follow these steps to attach a PC or terminal to the console port or Ethernet port.

1. Connect a PC or terminal to the console port or Ethernet port using the appropriate cable.
2. Open the terminal emulation program, and set the session parameters as follows:
   - Baud: 9600 bps
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

Activating the power source

When you complete the hardware installation, you are ready to activate the power source.

1. Verify that all modules and power supplies are properly installed and all empty slots are covered by slot blanks.

   CAUTION
   If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

2. If you are supplying a DC power source to your router, attach a power cable to each installed DC power supply as described in the appropriate section:

   Connect the other end of each cable to the DC power source. When you have completed these steps for each power supply you can activate the power source.

3. If you are supplying AC power to your router, attach one end of an AC power cord to each installed AC power supply as described in the appropriate section:

   Insert the other end of each cable into a wall outlet. The following rules apply:

   - 1200W power supplies require 115V/120V outlets.
   - 1800W power supplies require 200V-240V for full power or are limited to 1200W with 115V/120V outlets.
   - 2400W and 3000W power supplies require high line (200V-240V) outlets.

   DANGER
   If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

   NOTE
   Because the router is designed to provide uninterrupted service even when you insert or remove management modules and interface modules, there is no on/off power switch. To turn the system off, simply unplug the power cords.

   NOTE
   Wall outlets should be installed near the equipment and should be easily accessible.

4. Verify that the router has initialized successfully. Refer to Verifying proper operation on page 172.

Verifying proper operation

To verify that your router is operating properly, observe the LEDs, or display the status of the modules using the CLI.

Observing the LEDs

When power is supplied to the router, you can observe the LEDs to verify that the router initialized successfully. The following table describes the LEDs, the desired state of each LED, possible abnormal states of each LED, and what to do if an LED indicates an abnormal state.

TABLE 35 Router LED states and actions

LED label	Desired state	Meaning	Abnormal state	Meaning or action
Management module				
Active	The Active LED on one of the installed management modules should be on.	The module is functioning as the active management module.	Off	Neither of the management modules is managing the switch fabric and interface modules. A problem may have occurred during initialization. Check your attached PC or terminal for possible error messages.
Pwr	On	The module is receiving power.	Off	The module is not receiving power. Check the following: • Make certain that the module is installed properly. For more information, refer to the module installation section in this chapter that applies to your router model. • If you are using AC power supplies, refer to the AC power supply LED information in this table for more information.
10/100/1000 Ethernet Port	On (green)	A link is established with the remote port.	Off	A link is not established with the remote port. Check the following: • Verify that the connection to the other router has been properly made. Also, make certain that the other router is powered on and operating correctly. • Try using a different cable.
10/100/1000 Ethernet Port	On or blinking (yellow)	The port is transmitting and receiving packets.	Off for an extended period	The port is not transmitting or receiving packets. Check the following: • Look at the LED for the other 10/100/1000 Ethernet port to see if a link has been established with the remote port.

TABLE 35 Router LED states and actions (continued)

LED label	Desired state	Meaning	Abnormal state	Meaning or action
				• Verify that the connection to the other router has been properly made. Also, make certain that the other router is powered on and operating correctly. • Try using a different cable.
Interface module				
Pwr	On	The module is receiving power.	Off	The module is not receiving power. Check the following: • Make certain that the module is installed properly. For more information, refer to the module installation section in this chapter that applies to your router model. • The module may not be receiving enough power. Extreme recommends installing power supplies in a fully redundant configuration as described for each router model in this chapter. • Check the Pwr LED on the management module. If it is on, the management module may be preventing power from getting to the interface module. • Enter the **show chassis** command at any level of the CLI to determine if the management module recognizes the

TABLE 35 Router LED states and actions (continued)

LED label	Desired state	Meaning	Abnormal state	Meaning or action
				presence of all power sources. • If you are using AC power supplies, see the entry for the AC power supply LED in this table for more information.
Mgmt Act	During initialization: steady blinking.After initialization: occasional blinking.	The active management module processor and the interface module processor are communicating.	Off for an extended period.	The interface module may be in interactive mode. Check the status of the module by entering the **show module** command at any level of the CLI.
Link	On	A link is established with the remote port.	Off	This LED will remain off until you have cabled the interface module ports. After cabling the ports, if this LED is still off, a link is not established with the remote port.
Active	On or blinking	The port is transmitting and receiving user packets.	Off for an extended period.	This LED will remain off until you have cabled the interface module ports. After cabling the ports, if this LED is still off, the port is not transmitting or receiving user packets.
Switch Fabric module				
Pwr	On	The module is receiving power.	Off	The module is not receiving power. Check the following: • Make certain that the module is installed properly. For more information, refer to the module installation section in this chapter that applies to your router model. • If you are using AC power supplies, refer to the AC power supply LED information in this table for more information.
Active	On	The switch fabric module is active and ready to switch user packets.	Off for an extended period.	The switch fabric module is not active and user packets are not being switched from

TABLE 35 Router LED states and actions (continued)

LED label	Desired state	Meaning	Abnormal state	Meaning or action
				one interface module to another. You must replace the switch fabric module. Refer to Replacing a switch fabric module on page 248.
AC power supplies				
AC OK	Green (steady)	The power supply is receiving power from the AC power source.	Off	The power supply is not receiving power from an AC power source You can do the following: • Make sure that the power cord is connected securely to the wall outlet and the power supply. • Make sure that the wall outlet is rated for 115/120V and 20A. If it is not, obtain a cable that is rated for the outlet. • Make sure that the wall outlet has power.
DC OK	Green (steady)	The power supply is providing AC power to the router.	Off	The power supply is not supplying power to the router. If the AC LED is green, there is a problem with the power supply and it must be replaced.
ALM	Off	The power supply is in normal operating condition.	Amber	The power supply is malfunctioning.
DC power supplies				
DC IN	Green (steady)	The power supply is receiving power from the DC power source.	Off	The power supply is not receiving power from a DC power source You can do the following: • Make sure that the power supply cables are connected securely to the power source and the power supply. • Make sure the wall outlet is rated for high line, 200-240 VAC and 20A. If it is not obtain a cable

TABLE 35 Router LED states and actions (continued)

LED label	Desired state	Meaning	Abnormal state	Meaning or action
				that is rated for the outlet. • Make sure that the power source has power.
DC OUT	Green (steady)	The power supply is providing DC power to the router.	Off	The power supply is not supplying power to the router. If the DC IN LED is green, then there is a problem with the power supply and it must be replaced.
ALM	Off	The power supply is in normal operating condition.	Amber	The power supply is malfunctioning.
Fan control module (two LEDs on rear panel of router)				
Unlabeled	Green (steady)	The fans are working and responding to controls from the fan control module.	Off or amber	The fans are not receiving power (off), or the fans are not working and not responding to controls from the fan control module (amber). Check the following: • If the LED is off, check the power LED on the other modules to make sure they are receiving power. If you are using a DC power source, check your power source for problems. • If you are using AC power supplies, take the actions described in the Meaning or Action column for the AC power supply LED. If these actions do not resolve the problem, check the LED on each power supply or enter the **show chassis** command at any CLI prompt to determine if a power supply has failed. If a power supply has failed, you must replace it.

TABLE 35 Router LED states and actions (continued)

LED label	Desired state	Meaning	Abnormal state	Meaning or action
				• If the LED is amber, you must replace the fan module.

NOTE
If a problem persists after taking the actions described in this table, contact technical support.

Displaying the module status

After you have attached a PC or terminal to the console port or Ethernet port on the management module and the router has initialized successfully, press **Enter** to display the CLI prompt in the terminal emulation window. This example is a prompt for a 16-slot router.

```
device>
```

If you do not see this prompt, check the following items.

1. Make sure the cable is securely connected to your PC or terminal and the console port or Ethernet port.

2. Check the settings in your terminal emulation program. In addition to the session settings listed in Attaching a PC or terminal to the console port or Ethernet port on page 171, make sure the terminal emulation session is running on the same serial port you attached to the console port.

   When you see this prompt (MLX-16# or MLX-32#), you are connected to the system and can display module status using the CLI. Enter the **show module** command at any CLI level.

```
MLX-32# show module
Module Status Ports Starting MAC
M1 (upper): MLX Series Mgmt Module Active
M2 (lower):
F0: MLX Series Switch Fabric Module Active
S1:
S2:
S3:
S4: MLX Series 4-Port 10Gig Module CARD_STATE_UP 4 000c.db80.0000
S5: MLX Series 4-Port 10Gig Module CARD_STATE_UP 4 000c.db80.0000
S6: MLX Series 4-Port 10Gig Module CARD_STATE_UP 4 000c.db80.0000
S7:
S8:
```

   The Status column shows the module status. The management module status can be one of the following:

   - `ACTIVE` - The module is currently the active management module.
   - `STANDBY` - The module is currently the standby management module.
   - `COMING UP` - The module is coming up as the standby module. This status occurs if the standby management module becomes the active module during a switch over.

   The switch fabric module status can be one of the following:

   - `ACTIVE` - The module is up and running.
   - `BAD` - The management module cannot initialize the switch fabric module.

   An interface module status can be one of the following:

   - `CARD_STATE_INIT` - The system detects the module but the module is not up and running yet.
   - `CARD_STATE_BOOT` - The module is booting.
   - `CARD_STATE_INTERACTIVE` - The module is booting from interactive mode.
   - `CARD_STATE_LP_SYNC` - The software images are synchronized between the management module and interface module.
   - `CARD_STATE_SYNC` - The system is currently synchronizing the software image between the management module and interface module.
   - `CARD_STATE_SOFTWARE_LOADED` - The module has loaded the software image.
   - `CARD_STATE_POWER_OFF` - The module does not have power.
   - `CARD_STATE_UP` - The module is operating normally.
   - `CARD_STATE_FAILED` - The management module was unable to bring up an interface module. If you see this status, make certain that the interface module is installed properly. For more information, refer to Installing the MLXe-16 router modules on page 115 or Installing modules in the MLXe-32 router on page 152.
   - `CARD_DOWN_REASON_` *explanation* - The module is in a nonfunctional state. This status appears with an explanation for why the module is down. For example, `CARD_DOWN_REASON_BOOT_FAILED`. If the explanation does not help you resolve the problem, contact technical support and provide the explanation included with this status.

Forced card deletion

This feature allows you to remove a module configuration from the running configuration in interactive mode, while a different module is inserted. Users should copy the configuration of the existing module (if applicable) before performing the following steps.

1. (Optional) Copy the running configuration of the existing module interfaces to a text editor, if the new module requires the existing configuration. The configuration for the existing module will be automatically removed from the running configuration after you enter the **no module** command as shown in the following steps.
2. Remove the existing module, and insert the new module.
   The new module should come up in interactive state, and can be code synced at this time if needed.
3. Enter configuration mode.
4. Execute the following command:

   ```
   device(config)#no module <slot> <module-type>
   ```

   Example:

   ```
   device(config)#no module 2 ni-mlx-8-port-10g-d
   ```

   NOTE
   This is best pulled directly from the running configuration.

5. Answer "yes" to the prompt by pressing **y** .
6. Wait for the new module to come up.
7. Apply the appropriate configuration to the interfaces of the new module.

8. Enter the **write memory** command to save the new configuration.

   The following example demonstrates the forced card deletion feature:

```
device#show module
Module                                    Status       Ports  Starting MAC
M1 (left):BR-MLX-MR2-M Management Module  Active
M2 (right):NI-MLX-MR Management Module    Standby(Ready State)
F1:
F2: NI-X-HSF Switch Fabric Module         Active
F3: NI-X-HSF Switch Fabric Module         Active
S1: BR-MLX-40Gx4-M 4-port 40GbE Module    CARD_STATE_UP  4    0024.3887.3f00
S2: NI-MLX-10Gx8-D 8-port 10GbE (D) Module CARD_STATE_UP  8    0024.3887.3f30
S3: NI-MLX-10Gx8-D 8-port 10GbE (D) Module CARD_STATE_UP  8    0024.3887.3f60
S4: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.3f90
S5: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.3fc0
S6: NI-MLX-1Gx20-GC 20-port 10/100/1000
Copper Module                             CARD_STATE_UP  20   0024.3887.3ff0
S7: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.4020
S8: BR-MLX-40Gx4-M 4-port 40GbE Module    CARD_STATE_UP  4    0024.3887.4050
device#
device#show running-config | include module
module 1 br-mlx-4-port-40g-m
module 2 ni-mlx-8-port-10g-d
module 3 ni-mlx-8-port-10g-d
module 4 ni-mlx-8-port-10g-m
module 5 ni-mlx-8-port-10g-m
module 6 ni-mlx-20-port-1g-copper
module 7 ni-mlx-8-port-10g-m
module 8 br-mlx-4-port-40g-m
snmp-server max-ifindex-per-module 64
```

NOTE

At this stage of the process, the module is physically swapped.

```
device#show module
Module                                    Status       Ports  Starting MAC
M1 (left ):BR-MLX-MR2-M Management Module Active
M2 (right):NI-MLX-MR Management Module    Standby(Ready State)
F1:
F2: NI-X-HSF Switch Fabric Module         Active
F3: NI-X-HSF Switch Fabric Module         Active
S1: BR-MLX-40Gx4-M 4-port 40GbE Module    CARD_STATE_UP  4    0024.3887.3f00
S2: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_INTERACTIVE
    (S2: Configured as NI-MLX-10Gx8-D 8-port 10GbE (D) Module)
S3: NI-MLX-10Gx8-D 8-port 10GbE (D) Module CARD_STATE_UP  8    0024.3887.3f60
S4: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.3f90
S5: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.3fc0
S6: NI-MLX-1Gx20-GC 20-port 10/100/1000
Copper Module                             CARD_STATE_UP  20   0024.3887.3ff0
S7: NI-MLX-10Gx8-M 8-port 10GbE (M) Module CARD_STATE_UP  8    0024.3887.4020
S8: BR-MLX-40Gx4-M 4-port 40GbE Module    CARD_STATE_UP  4    0024.3887.4050
device#configure terminal
device(config)#no module 2 ni-mlx-8-port-10g-d
```

NOTE

This command pertains to the output of the command **show running-config** previously executed.

```
Removing module configuration requires power cycle of the module, to bring back the module to UP
state. Do you want to continue?
(enter 'y' or 'n'): y
Reset slot 2
device(config)#end
device#
device#show module
Module                                    Status       Ports  Starting MAC
M1 (left ):BR-MLX-MR2-M Management Module Active
M2 (right):NI-MLX-MR Management Module    Standby(Ready State)
F1:
F2: NI-X-HSF Switch Fabric Module         Active
```

```
F3: NI-X-HSF Switch Fabric Module            Active
S1: BR-MLX-40Gx4-M 4-port 40GbE Module       CARD_STATE_UP  4   0024.3887.3f00
S2: NI-MLX-10Gx8-M 8-port 10GbE (M) Module   CARD_STATE_UP  8   0024.3887.3f30
S3: NI-MLX-10Gx8-D 8-port 10GbE (D) Module   CARD_STATE_UP  8   0024.3887.3f60
S4: NI-MLX-10Gx8-M 8-port 10GbE (M) Module   CARD_STATE_UP  8   0024.3887.3f90
S5: NI-MLX-10Gx8-M 8-port 10GbE (M) Module   CARD_STATE_UP  8   0024.3887.3fc0
S6: NI-MLX-1Gx20-GC 20-port 10/100/1000
Copper Module                                CARD_STATE_UP  20  0024.3887.3ff0
S7: NI-MLX-10Gx8-M 8-port 10GbE (M) Module   CARD_STATE_UP  8   0024.3887.4020
S8: BR-MLX-40Gx4-M 4-port 40GbE Module       CARD_STATE_UP  4   0024.3887.4050
device#show running-config | include module
module 1 br-mlx-4-port-40g-m
module 2 ni-mlx-8-port-10g-m
module 3 ni-mlx-8-port-10g-d
module 4 ni-mlx-8-port-10g-m
module 5 ni-mlx-8-port-10g-m
module 6 ni-mlx-20-port-1g-copper
module 7 ni-mlx-8-port-10g-m
module 8 br-mlx-4-port-40g-m
snmp-server max-ifindex-per-module 64
device#
```

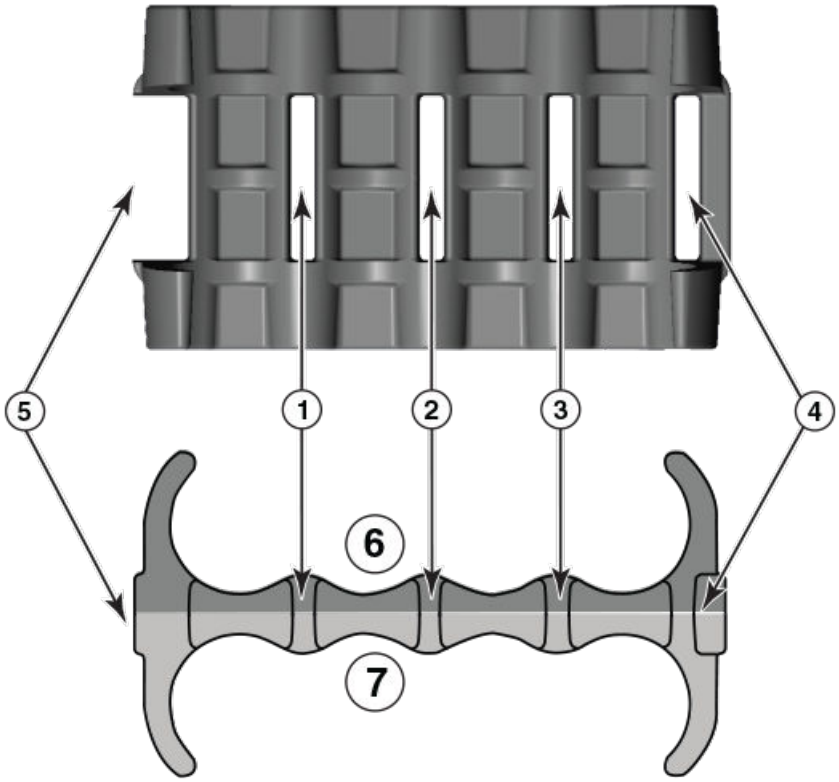
Using Extreme Structured Cabling Components

- Cable cinch overview....183
- mRJ21 procedures....184
- RJ-45 procedures....187

Cable cinch overview

Position the cable cinch with the open end to the left (no slot), as shown in the following figure.

FIGURE 91 Cable cinch overview



1	Slot 1	5	Slot 3
2	Open end	6	Front
3	Slot 2	7	Slot 4
4	Rear		

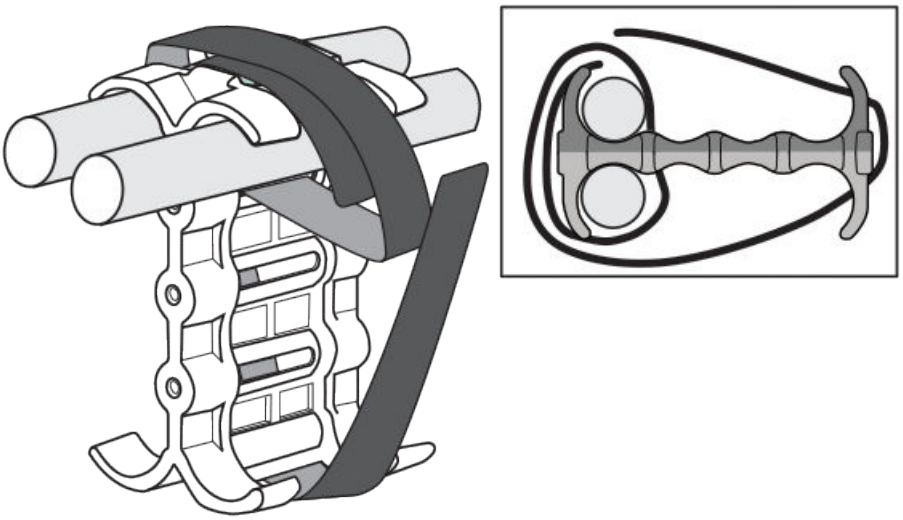
mRJ21 procedures

The following procedure demonstrates securing up to eight mRJ21 cables into the cable cinch. When securing fewer than the maximum cables, follow the procedure to secure the desired number of cables and simply wrap the remaining Velcro strap around the cable cinch. Use the additional slots in the clip to secure groups of cables as required.

Cable cinch with two mRJ21 cables

To secure two mRJ21 cables, place the Velcro strap through slot one and use the front and rear left recesses as shown in the following figure.

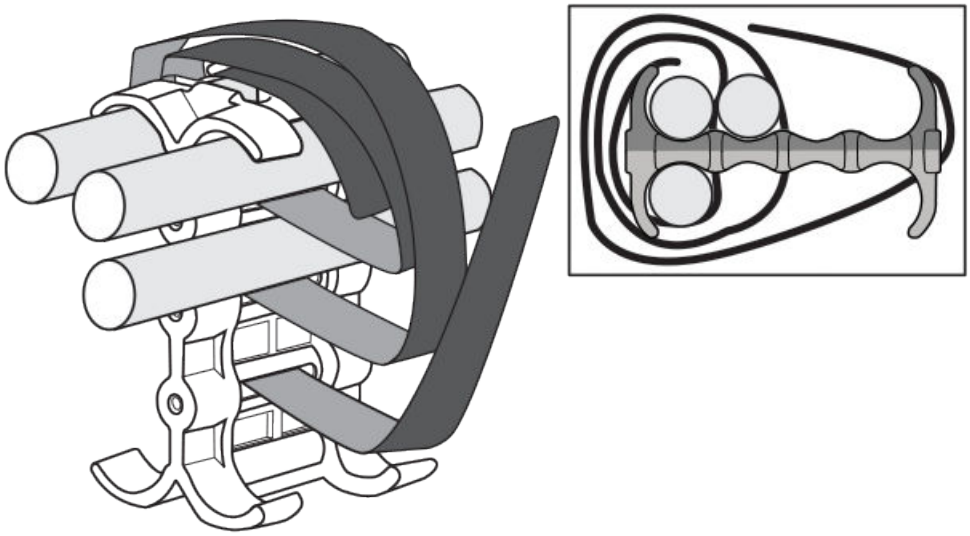
FIGURE 92 Two mRJ21 cables



Cable cinch with three mRJ21 cables

Three mRJ21 cables may be secured as shown in the following figure.

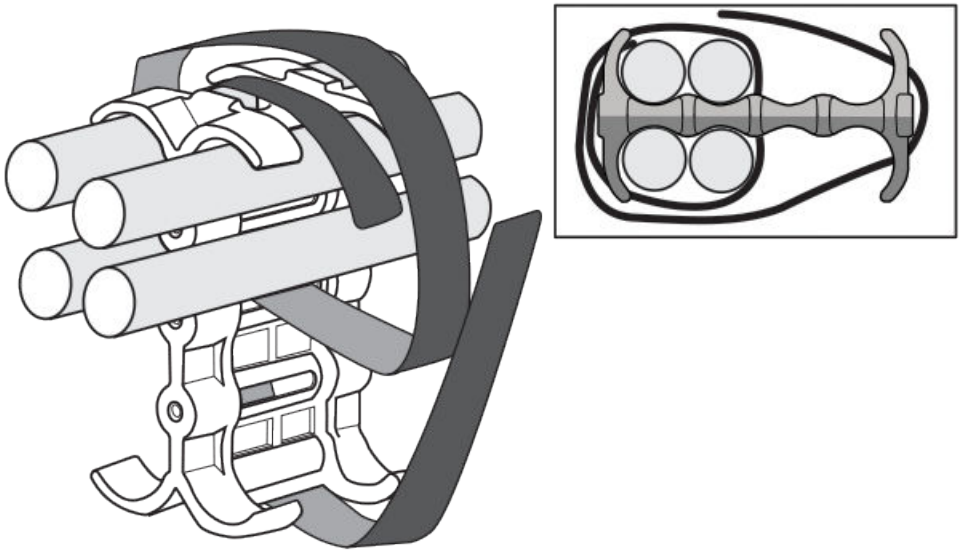
FIGURE 93 Three mRJ21 cables



Cable cinch with four mRJ21 cables

Four mRJ21 cables may be secured as shown in the following figure.

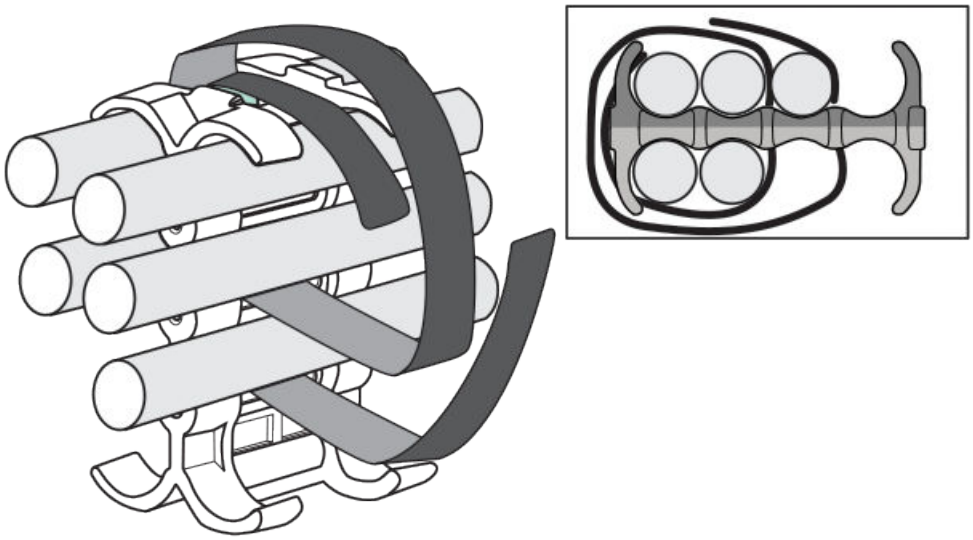
FIGURE 94 Four mRJ21 cables



Cable cinch with five mRJ21 cables

Five mRJ21 cables may be secured as shown in the following figure.

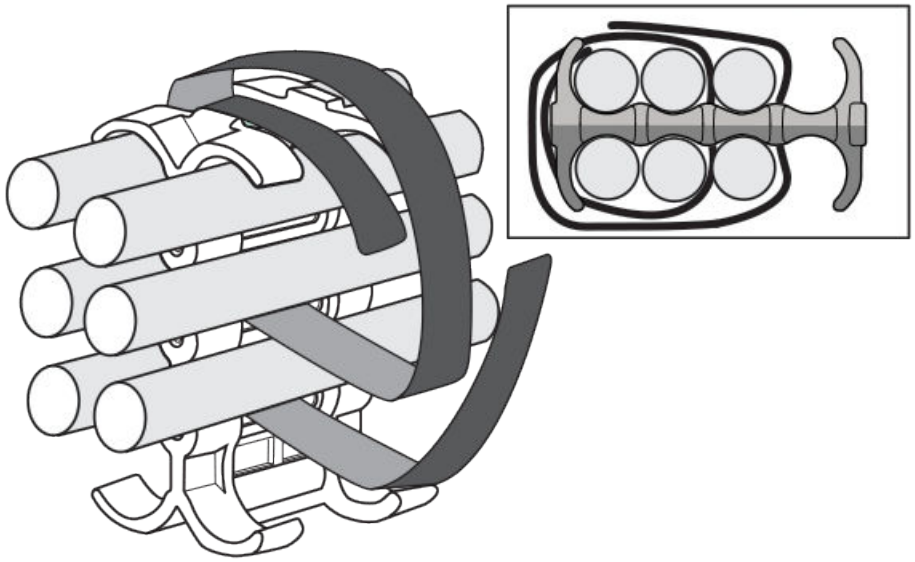
FIGURE 95 Five mRJ21 cables



Cable cinch with six mRJ21 cables

Six mRJ21 cables may be secured as shown in the following figure.

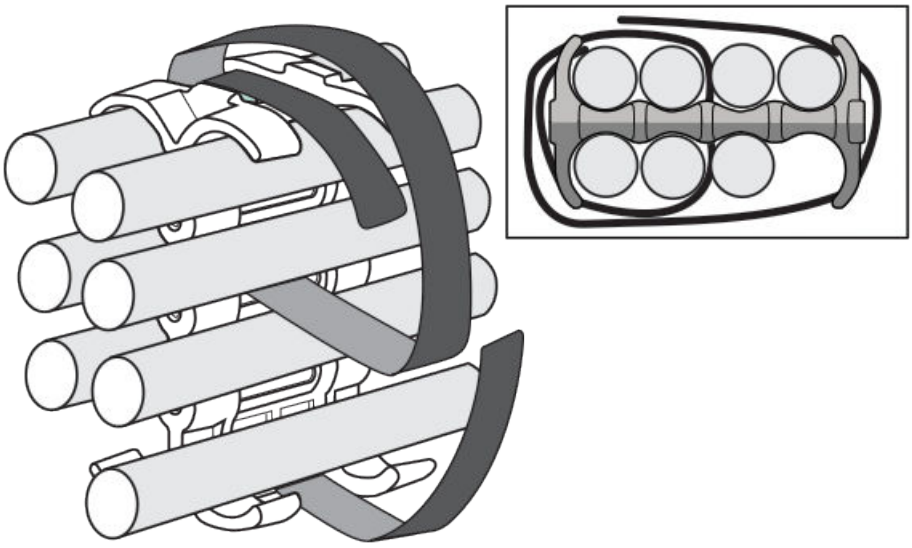
FIGURE 96 Six mRJ21 cables



Cable cinch with seven mRJ21 cables

Seven mRJ21 cables may be secured as shown in the following figure.

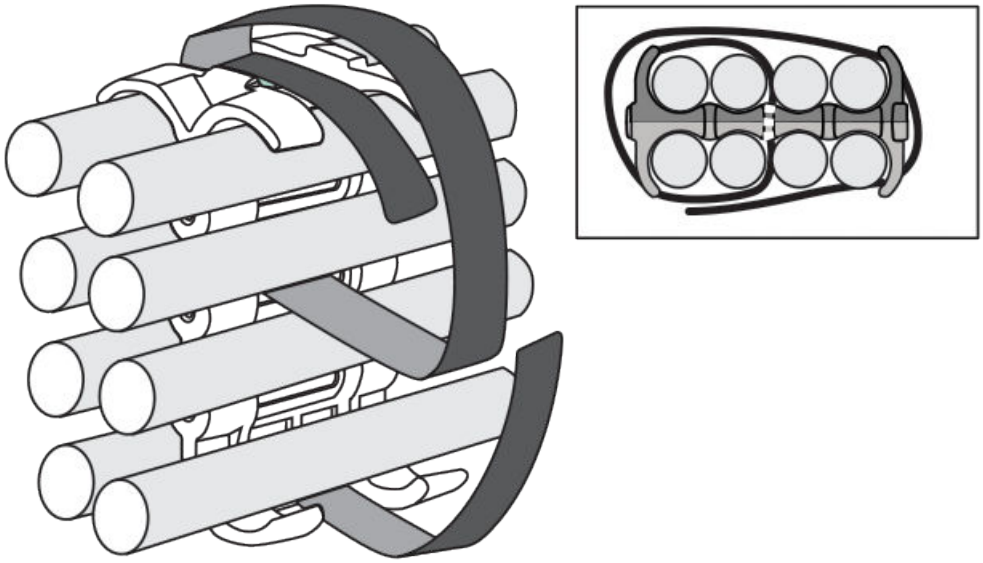
FIGURE 97 Seven mRJ21 cables



Cable cinch with eight mRJ21 cables

Eight mRJ21 cables may be secured as shown in the following figure.

FIGURE 98 Eight mRJ21 cables



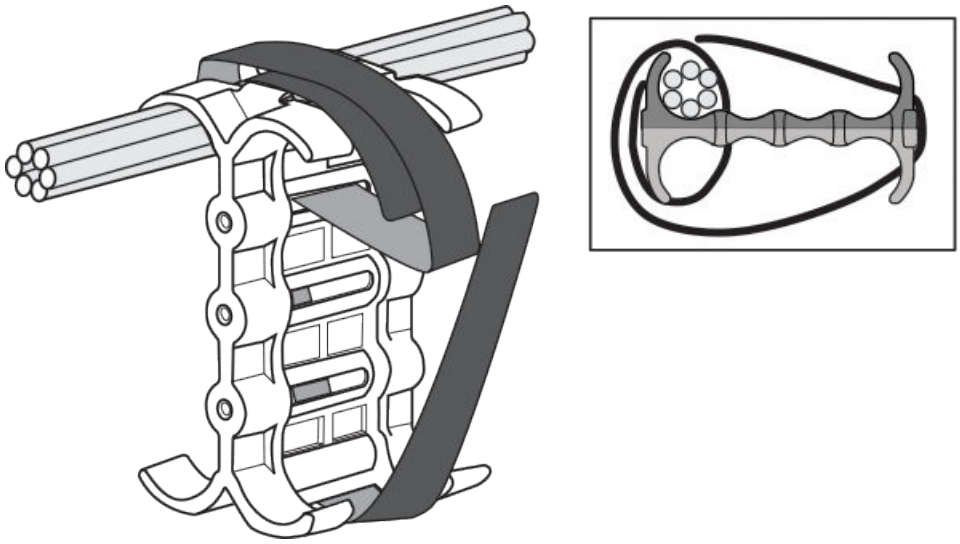
RJ-45 procedures

Use the following guidelines when using the cable cinch clips with RJ-45 cables.

Cable cinch with one group of RJ-45 cables

RJ-45 cables may be secured in groups of six. To secure up to six RJ-45 cables in one group, place the Velcro strap through slot one and use the front left recesses as shown in the following figure.

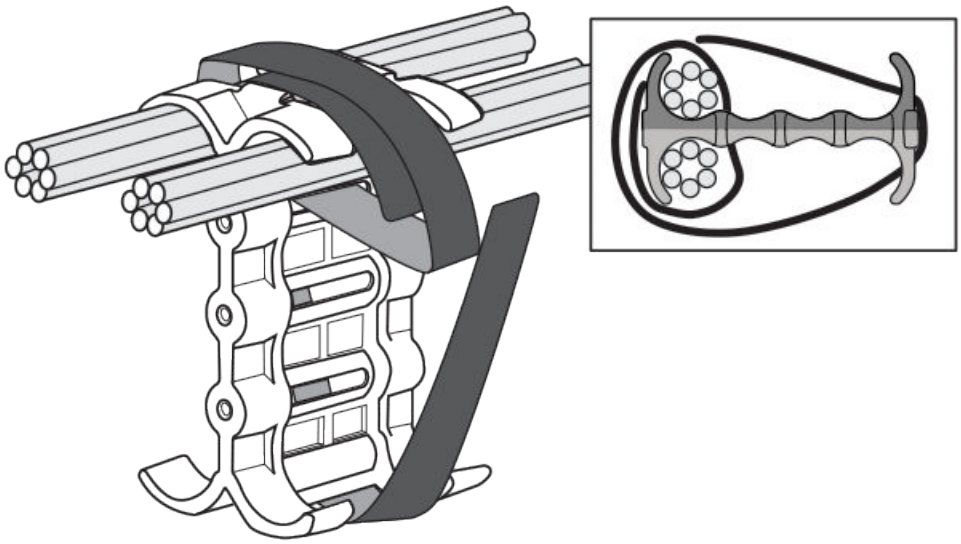
FIGURE 99 One group of RJ-45 cables



Cable cinch with two groups of RJ-45 cables

12 RJ-45 cables, in two groups, may be secured as shown in the following figure.

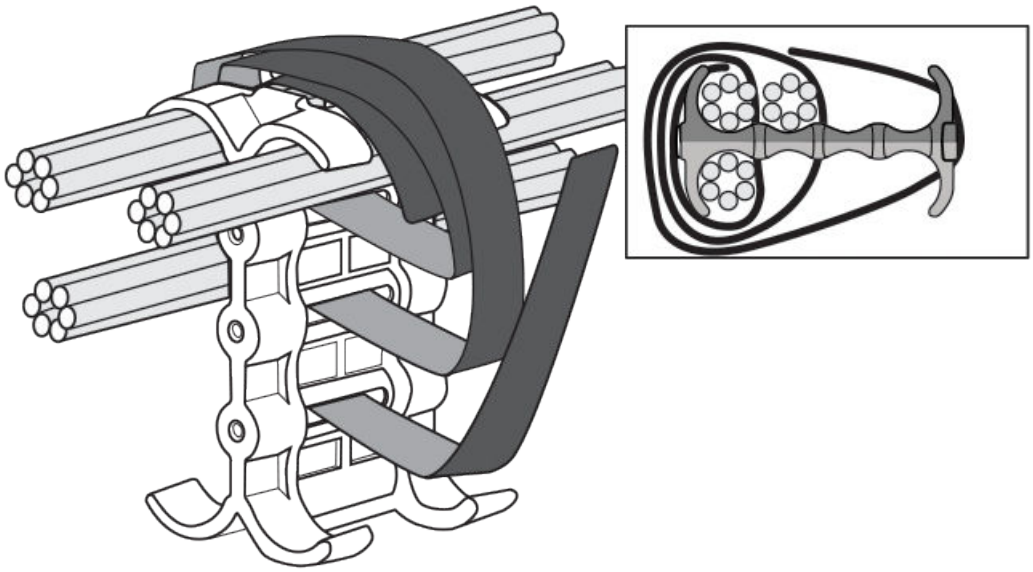
FIGURE 100 12 RJ-45 cables in two groups



Cable cinch with three groups of RJ-45 cables

18 RJ-45 cables, in three groups, may be secured as shown in the following figure.

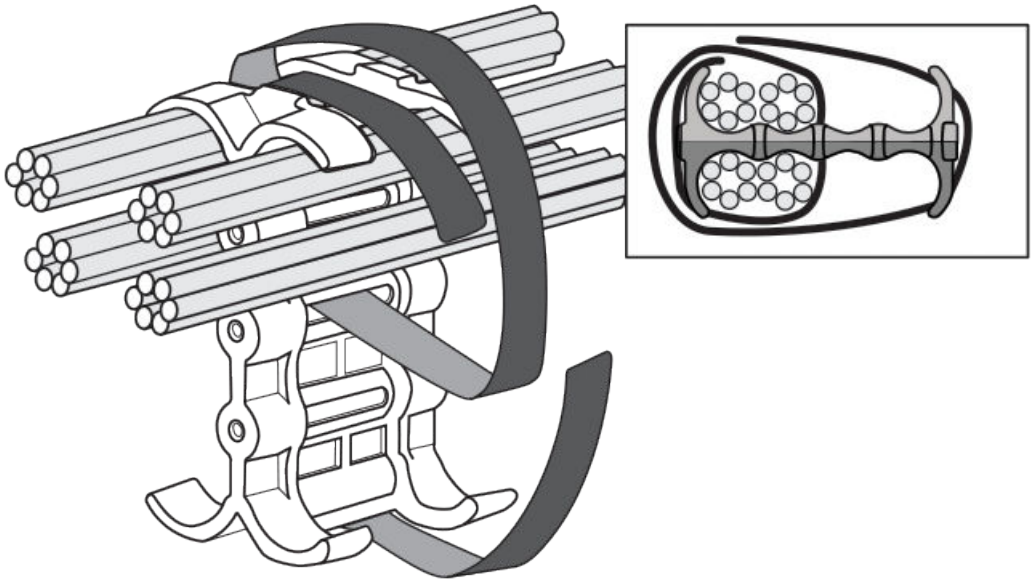
FIGURE 101 18 RJ-45 cables in three groups



Cable cinch with four groups of RJ-45 cables

24 RJ-45 cables, in four groups, may be secured as shown in the following figure.

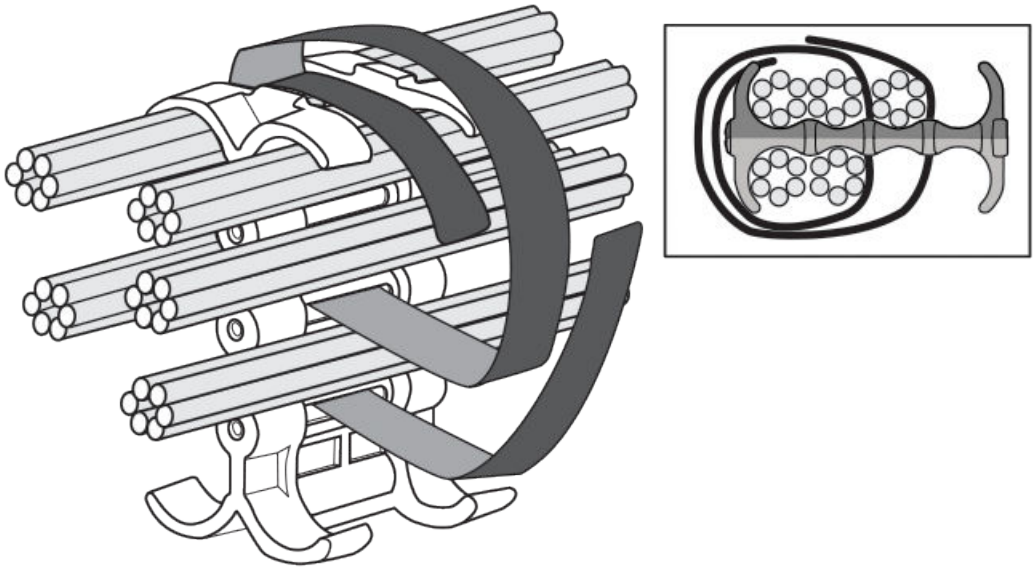
FIGURE 102 24 RJ-45 cables in four groups



Cable cinch with five groups of RJ-45 cables

30 RJ-45 cables, in five groups, may be secured as shown in the following figure.

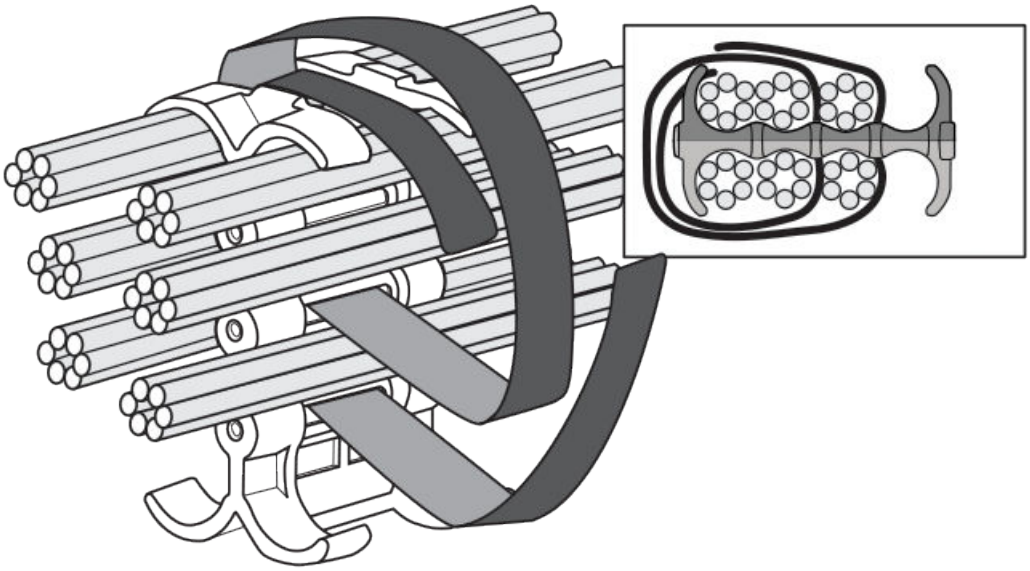
FIGURE 103 30 RJ-45 cables in five groups



Cable cinch with six groups of RJ-45 cables

36 RJ-45 cables, in six groups, may be secured as shown in the following figure.

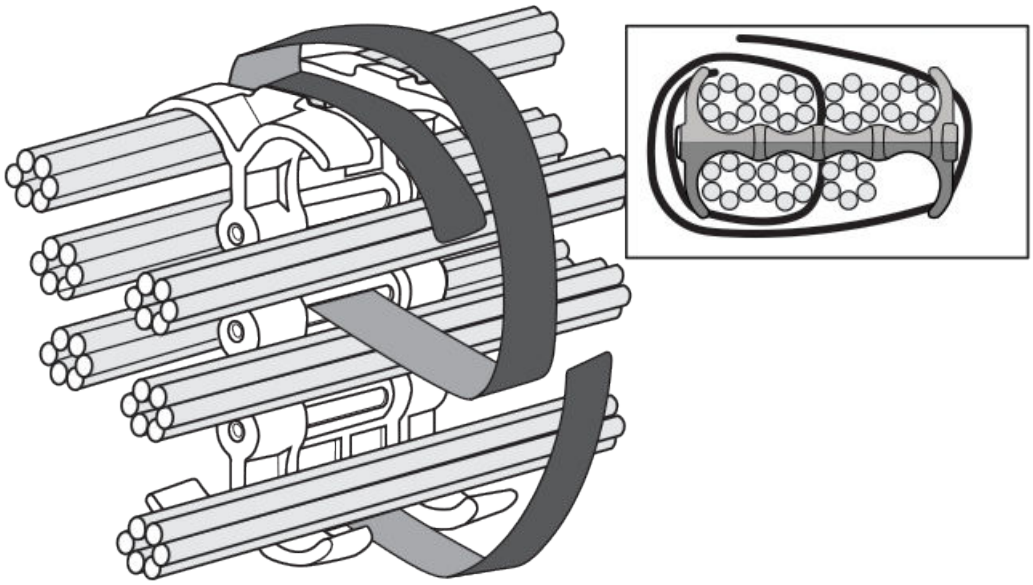
FIGURE 104 36 RJ-45 cables in six groups



Cable cinch with seven groups of RJ-45 cables

42 RJ-45 cables, in seven groups, may be secured as shown in the following figure.

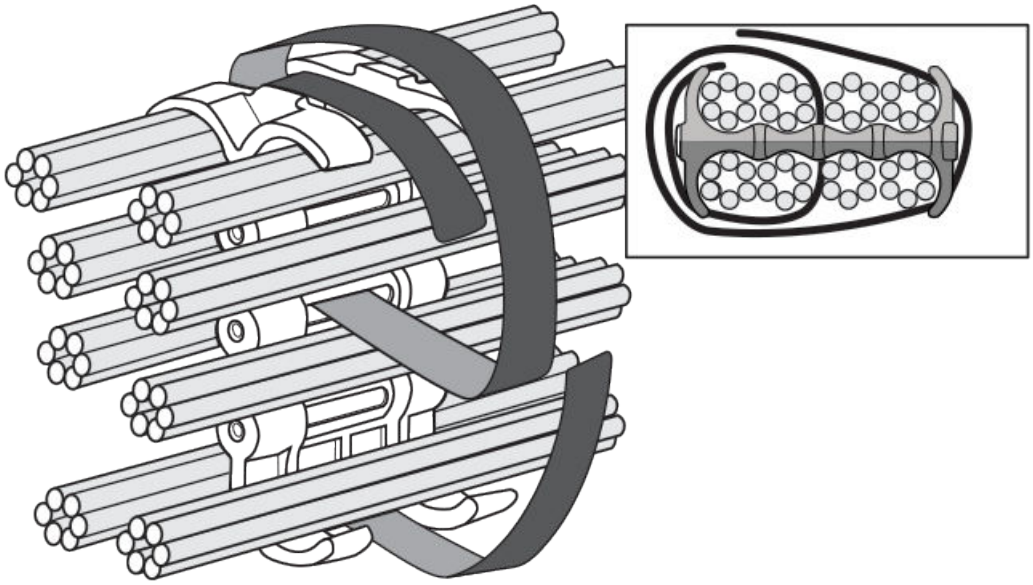
FIGURE 105 42 RJ-45 cables in seven groups



Cable cinch with eight groups of RJ-45 cables

48 RJ-45 cables, in eight groups, may be secured as shown in the following figure.

FIGURE 106 48 RJ-45 cables in eight groups



Connecting a Router to a Network Device

- Assigning permanent passwords....193
- Configuring IP addresses....194
- Understanding management port functions....196
- Connecting the router to a network device....197
- Testing network connectivity....200

Assigning permanent passwords

DANGER
The procedures in this manual are for qualified service personnel.

By default, the CLI is not protected by passwords. To secure CLI access, it is strongly recommended that you assign passwords.

The CLI contains the following access levels:

- Privileged EXEC - This level is also called the Enable level and can be secured by a password. From this level you can manage files on the management module flash memory or a auxiliary flash card in the management module slots 1 or 2, save the system configuration to flash memory, and clear caches.
- CONFIG - The configuration level. From this level you can configure a system IP address and configure routing features. To access the CONFIG mode, you must already be logged into the Privileged level of the EXEC mode.

  NOTE
  You cannot assign a password using the Web management interface. You can assign passwords using the Extreme Network Advisor software if an Enable password for a super user is already configured on the device.

You can set the following levels of Enable passwords:

- Super user - Allows complete read-and-write access to the system. This is generally for system administrators and is the only password level that allows you to configure passwords.

  NOTE
  You must set a super-user password before you can set other types of passwords.

- Port configuration - Allows read-and-write access for specific ports but not for global (system-wide) parameters.
- Read only - Allows access to the Privileged EXEC mode and CONFIG mode but only with read access.

To set passwords, perform the following steps:

1. At the opening CLI prompt, enter **enable** to change to the Privileged level of the EXEC mode.

   ```
   device enable
   device#
   ```

2. Access the CONFIG level of the CLI by entering the **configure terminal** command.

   ```
   device# configure terminal
   device(config)#
   ```

3. Enter the **enable super-user-password** command to set the super-user password.

```
device(config)#
         enable super-user-password mustang
```

NOTE
You must set the super-user password before you can set other types of passwords.

4. Enter the following commands to set the port configuration and read-only passwords.

```
device(config)#         enable port-config-password mustang
device(config)#         enable read-only-password mustang
```

NOTE
If you forget your super-user password, refer to the release notes.

The text for the **read-only--password** and the **port-config password** should be different from the text for the super-user password. Passwords can be up to 48 characters long.

Configuring IP addresses

Extreme routers implement separate data and control planes. This architecture affects how you assign IP addresses. The following table outlines the interfaces to which you can assign IP addresses.

In this table, "In band" refers to an interface over which user packets are routed, while "Out of band" refers to an interface over which control packets related to system management are forwarded.

TABLE 36 Interfaces that can be given IP addresses

Interface	Associated physical port	Out of band or In band
Management interface	Ethernet 10/100/1000 port on active or redundant management module	Out of band
Any interface over which user packets are routed	Any interface module port	In band
Any virtual interface over which user packets are routed	Any interface port	In band
Loopback interface	-	In band

Support of subnet masks

Extreme routers support both classical IP network masks (Class A, B, and C subnet masks, and so on) and Classless Interdomain Routing (CIDR) network prefix masks.

- Enter a classical network mask in IP address format. For example, enter "209.157.22.99 255.255.255.0" for an IP address with a Class-C subnet mask.
- To enter a prefix number for a network mask, enter a forward slash (/) and the number of bits in the mask immediately after the IP address. For example, enter "209.157.22.99/24" for an IP address that has a network mask with 24 significant ("mask") bits.

Assigning an IP address to a management interface

Instead of assigning a global IP address to the router for system management purposes, you must assign an IP address to the active management module. If the active management module becomes unavailable and the redundant module becomes the active module, the IP address is automatically assigned to the new active management module.

For example, to assign the IP address 10.0.1.1 to the management module, use these steps.

1. At the opening CLI prompt, enter **enable** .

```
device# enable
```

2. Enter the **erase startup-config** command at the Privileged EXEC level prompt (for example, device#), then press **Enter**. This command erases the factory test configuration if it is still present.

```
device# erase startup-config
```

After entering this command, perform a reload on the system.

CAUTION
Use the erase startup-config command only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally do erase the configuration on a configured system, enter the write memory command to save the running configuration to the startup-config file.

3. Access the configuration level of the CLI by entering the **configure terminal** command.

```
device# configure terminal
device(config)#
```

4. Configure the IP address and mask for the management interface by entering these commands.

```
device(config)# interface management 1
device(config-if-mgmt-1)# ip address 10.0.1.1 255.255.255.0
```

or

Assigning IP addresses to an interface, virtual interface,or loopback interface

You must assign an IP address to each interface and virtual interface over which user packets are routed. You can also assign an IP address to a loopback interface, which is generally used for testing and diagnostic purposes.

You must use the serial connection to assign the first IP address. For subsequent addresses, you can also use the CLI through Telnet or the Web management interface. Use Extreme Network Advisor to assign IP addresses to virtual routing interfaces only.

By default, you can configure up to 24 IP addresses on each interface, virtual interface, and loopback interface.

For example, to assign the IP address 192.22.3.44 and subnet mask 255.255.255.0 to Ethernet interface 1/1, do the following.

1. At the opening CLI prompt, enter **enable** .

```
device# enable
```

2. Enter the following command at the Privileged EXEC level prompt, then press **Enter** . This command erases the factory test configuration if it is still present.

```
device# erase startup-config
```

After you enter this command, you will need to restart the system.

CAUTION
Use the erase startup-config command only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally erase the configuration on a configured system, enter the write memory command to save the running configuration to the startup-config file.

3. Access the configuration level of the CLI by entering the following command.

```
device# configure terminal
device(config)#
```

4. Configure the IP address and subnet mask for Ethernet interface 1/1 by entering the following commands.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip address 192.22.3.44 255.255.255.0
```

Syntax: enable [*password*]

Syntax: configure terminal

Syntax: [no] ip address *ip-addrip-mask* [**secondary**]

or

Syntax: [no] ip address *ip-addr/mask-bits* [**secondary**]

Use the *secondary* parameter if you have already configured an IP address within the same sub-net on the interface.

Enabling and disabling the interfaces

By default, all router interfaces are disabled. To enable an interface, enter the **enable** command at the appropriate interface configuration level of the CLI. For example, to enable the management interface, enter the **enable** command at the management interface configuration level of the CLI.

```
device(config-if-mgmt-1)# enable
```

You can disable each of these interfaces using the **disable** command at the appropriate interface configuration level of the CLI. For example, to disable the management port, enter the **disable** command at the management interface configuration level of the CLI.

```
device(config-if-mgmt-1)# disable
```

Understanding management port functions

The management port performs specific functions and is subject to some limitations, as described.

- Because the management port allows you to configure, monitor, and manage routers only, this port has the same limited functionality as an IP host port.
- You cannot enable and run routing protocols on the management port.
- You cannot configure routes from the management interface.
- The management port uses static IP routes from the interface routing tables.

- If you configure the redistribution of static or directly connected routes for a particular routing protocol, the protocol redistributes routes associated with the interface module ports, but not the routes associated with the management port.

To display configuration information and statistics about the management port, enter the **show interface management 1** command at any CLI level.

Connecting the router to a network device

You can connect a router to another Ethernet network device. MLX Series routers support connections to other vendors' devices as well as Extreme network devices.

The Ethernet interface modules available with the MLX Series routers are described in Connecting the router to a network device. These include XFP fiber, SFP and SFP+ fiber, and RJ45 copper interfaces. Details regarding the SFP, SFP+, and XFP fiber-optic transceivers supported for these interface modules are also described.

To connect a router to another network device, you must do the following.

- Install the fiber-optic modules if required.
- Cable the modules with either copper cable or fiber-optic cable as required.

The following sections provide information about module installation and cabling, as well as how to clean fiber-optic connectors and troubleshoot network connections.

Installing a fiber-optic transceiver

To connect a router to another network device using a fiber port, install a fiber-optic transceiver (SFP, SFP+, or XFP, as required by your interface module).

DANGER
All fiber-optic interfaces use Class 1 lasers.

NOTE
Refer to Installation precautions on page 87 for other hardware installation precautions.

Before installing a fiber-optic transceiver, have on hand an ESD wrist strap with a plug for connection to the ESD connector on the router chassis.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

Follow these steps to install a fiber-optic transceiver.

1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the router chassis.
2. Remove the transceiver from the protective packaging.
3. Remove the metal cover from the port on the interface module.
4. Gently insert the fiber-optic transceiver into the port until the transceiver clicks into place. Transceivers are keyed to prevent incorrect insertion.

Cabling a fiber-optic transceiver

Follow these steps to cable a fiber-optic transceiver.

1. Remove the protective covering from the fiber-optic port connectors and store the covering for future use.
2. Before cabling a fiber-optic transceiver, it is strongly recommended that you clean the cable connectors and the port connectors. For more information, refer to Cleaning fiber-optic ports and connectors on page 198.
3. Gently insert the two cable connectors (a tab on each connector should face upward) into the ports until the tabs lock into place.

Tunable 10 GbE DWDM SFP+

NOTE
Tunable 10 GbE DWDM SFP+ are only supported on MLX8x10, MLX24x10 modules

The tunable 10 GbE dense wavelength-division multiplexing (DWDM) SFP+ modular optic (part number 10G-SFPP-ZRD-T) can be configured through the CLI to use C-band channels 1 - 102 for flexible metro or campus Ethernet links that reach up to 80 km.

For 10-Gigabit Ethernet DWDM interfaces only, configure full C-band tunable optics as shown below.

To configure a physical port, enter a command such as the following.

```
device(config-if-e10000-1/1)# tunable-optic sfpp channel 5
```

To configure a LAG port, enter a command such as the following.

```
device(config-if-e10000-1/1)# physical-port 1/1 tunable-optic sfpp channel 5
device(config-lag-lag1)# physical-port 1/1 tunable-optic sfpp channel 5 show
Channel 5: 191.3THz, 1567.13nm
```

Use the *channel number* parameter to specify the channel number to use on the interface. Possible values 0 through 102.

Use the **show** options to display the SFPP channel used on the interface.

Cleaning fiber-optic ports and connectors

To avoid problems with connections between fiber-optic ports and fiber cable connectors, it is strongly recommended that you clean ports and connectors each time you make a connection. Dust can accumulate inside the port and connector and cause problems as serious as reducing the optic launch power.

To clean the fiber-optic ports and cable connectors, it is recommended that you use a fiber-optic reel-type cleaner. You can purchase this type of cleaner from the following website:

`http://www.fisfiber.com/`

When you are not using a fiber-optic transceiver port, always replace the protective cover.

Troubleshooting network connections

Observe connection LEDs to determine if network connections are functioning properly. Table 37 lists the LEDs related to the network connections, the desired state of each LED, possible abnormal states of each LED, and what to do if an LED indicates an abnormal state.

TABLE 37 Network connection-related LED states

LED	Desired state	Meaning	Abnormal state	Meaning or action
Interface module				

TABLE 37 Network connection-related LED states (continued)

LED	Desired state	Meaning	Abnormal state	Meaning or action
Link	On	A link is established with the remote port.	Off	A link is not established with the remote port. Try the following: • Verify that the connection to the other network device has been properly made, and that the other network device is powered on and operating correctly. • Verify that the transmit port on a router is connected to the receive port on the other network device, and that the receive port on the router is connected to the transmit port on the other network device. If you are not certain, remove the two cable connectors and reinsert them in the port connector, reversing their order. • Dust may have accumulated in the cable connector or port connector. For information about cleaning the connectors, refer to Cleaning fiber-optic ports and connectors on page 198. • If these actions do not resolve the problem, try using a different port or a different cable.
Active	On or blinking	The port is transmitting and receiving user packets.	Off for an extended period.	The port is not transmitting or receiving user packets. Try the following: • Check the Link LED to make sure the link is still

TABLE 37 Network connection-related LED states (continued)

LED	Desired state	Meaning	Abnormal state	Meaning or action
				established with the remote port. If not, take the actions described in the Meaning or Action column for the Link LED. • Verify that the port has not been disabled through a configuration change. You can use the CLI. If you have configured an IP address on the device, you also can use the Web management interface or Extreme Network Advisor.

NOTE
If a problem persists after taking these actions, contact Extreme Technical Support.

Testing network connectivity

After you cable the fiber-optic transceivers, you can test connectivity to other network devices by pinging those devices. You also can perform traceroutes.

Pinging an IP address

To verify that the router can reach another device through the network, enter a command such as the following at any level of the CLI.

```
device# ping 192.33.4.7
```

NOTE
If you send the ping to the IP broadcast address, the device lists the first four responses to the ping.

Tracing a route

To determine the path through which the router can reach another network device, enter a command such as the following at any level of the CLI.

```
device# traceroute 192.33.4.7
```

The CLI displays **traceroute** information for each hop on the route as soon as the information is received. **Traceroute** requests display all responses to a given TTL. If there are multiple equal-cost routes to the destination, the router displays up to three responses by default.

Managing Routers and Modules

- Managing the device....201
- Managing switch fabric modules....209
- Managing the cooling system....210
- Managing interface modules....218
- Monitoring Link Status....225
- Traffic Manager XPP link monitoring....226
- Using alarms to collect and monitor device status....228
- Displaying MR2 management module memory usage....232
- Enabling and disabling management module CPU usage calculations....233
- Displaying management module CPU usage....234
- Removing MAC address entries....235
- IPv6 ND Proxy....236
- DRBG Health Test on IPsec LP....243

Managing the device

You can perform these management tasks for the router:

- Enable and disable a DC power source, if necessary.
- Display status and temperatures of all hardware components.
- Display the Syslog configuration and static and dynamic buffers.
- Disable and re-enable power to interface modules.

Disabling and re-enabling power to interface modules

You can disable power and re-enable power to all interface modules, or to a specified interface module using the **power-off** command in the CLI, as shown in the following example:

```
device# power-off lp all
```

Syntax: power-off lp [**all**|*slot-number*]

- **all** - disables power to all interface modules
- *slot-number* - disables power to the interface module in the specified slot. You can specify 1-4 for 4-slot routers, 1-8 for 8-slot routers, 1-16 for 16-slot routers, and 1-32 for 32-slot routers.

  NOTE
  It is recommended that you do not disable power to interface modules during a software upgrade. If you try to disable power during a software upgrade, the following message will be displayed:`Warning: There is an outstanding software download.Do you want to continue ? (enter "y" or "n")` Type "**n** " and wait until the upgrade is complete.

To re-enable power to all interfaces or to a specific interface, enter the **power-on lp** command, as shown in this example:

```
device# power-on lp
```

Syntax: power-on lp [*slot-number*|**all**]

- **all** - enables power to all interface modules

- *slot-number* - disables power to the interface module in the specified slot. You can specify 1-4 for 4-slot routers, 1-8 for 8-slot routers, 1-16 for 16-slot routers, and 1-32 for 32-slot routers.

  NOTE
  There is a 10 second delay between the **power-off lp** command and the **power-on lp** command. Wait 10 seconds between commands.

Monitoring I2C failures on management modules

The management module accesses temperature sensors, fan controllers, power supplies, serial PROMs, and other devices are all accessed through the I2C serial bus. When I2C devices are inaccessible, generic (and uninformative) error messages are displayed on the management module console interface. If you do not keep a record of the console messages before the management module resets or reloads, these error messages will be lost.

At the first occurrence of an I2C failure, the Global I2C Error Indicator (GIEI) flag severity is set to major. The GIEI flag is cleared only when the management module is able to access the same physical device successfully. The GIEI severity flag is set to minor only if other I2C devices are accessible. A set of static and dynamic Syslog messages are generated when any or all of the following events occur:

- When an I2C failure is first detected
- When the GIEI severity is changed from major to minor
- When the GIEI flag is cleared

These Syslog messages are generated in both the static and dynamic sections of the **show logging** command output. A Syslog message is also sent to the SNMP log server.

When the GIEI is set to major, the first Syslog message displayed is an Alert. The following example shows an Alert Syslog message where the GIEI is set to major:

```
device# show logging
Sysloglogging: enabled (0 messages dropped, 0 flushes, 1 overruns)
Buffer logging: level ACDMEINW, 50 messages logged
level code: A=alert C=critical D=debugging M=emergency E=error
I=informational N=notification W=warning
Static Log Buffer:
Apr 16 18:21:25:A:System: Power Supply 2 , middle, Not Installed (FAILED)
Apr 16 18:21:25:A:System: Power Supply 3 , top, Not Installed (FAILED)
Apr 16 18:21:25:A:System: bad i2c access (GIEI = set), Severity Major
, Mux
index 0, Muxtap 4, ID 0x4, Addr0x5, (FANTRAY4)
Apr 16 18:21:25:I:System: last good i2c access, Muxindex 0, Muxtap 1, ID
0x9, Addr0x1, (SNM1TEMP)
Dynamic Log Buffer (50 lines):
Apr 16 18:21:25:A:System: bad i2c access (GIEI = set), Severity Major,
 Mux
index 0, Mux tap 4, ID 0x4, Addr 0x5, (FANTRAY4)
Apr 16 18:21:25:I:System: last good i2c access, Mux index 0, Mux tap 1, ID
0x9, Addr 0x1, (SNM1TEMP)
Mar 28 12:36:47:A:System: Set fan speed to MED (75%)
Mar 25 21:40:47:A:System: Set fan speed to MED-HI (90%)
```

The Syslog message shows the last successful I2C access by the management module and also contains the following information about the failed device:

- Current state of the GIEI flag
- Severity of the failure: major or minor
- MUX index number:
  - 0-1 - there are total of 2 MUX indexes in ExtremeRouting XMR Series 32000 and ExtremeRouting MLX-32 devices.
  - The MUX index is always zero in 4-, 8-, and 16-slot XMR Series or MLX Series devices

- MUX tap number:
  - 0-7 - there are total of 8 MUX taps connected to a MUX device.
  - 15 - MUX tap is non applicable
- Device ID
- Device address
- Description of the load

If the GIEI severity changes from the time the GIEI is set to major, the first Syslog message in the static section of the log is updated to reflect this change. A copy of this updated message is generated in the dynamic section of the log and a copy is sent to SNMP log server.

When an I2C failure is first detected, a second Syslog message is generated containing information about the last successful I2C access before the GIEI error flag was set. The last successful access information remains unchanged until the GIEI is cleared. A copy of the second Syslog message is also sent to the SNMP log server.

The second Syslog message is always displayed as an informational Syslog. The following example shows an informational Syslog message:

```
device# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 1 overruns)
Buffer logging: level ACDMEINW, 50 messages logged
level code: A=alert C=critical D=debugging M=emergency E=error
I=informational N=notification W=warning
Static Log Buffer:
Apr 16 18:21:25:A:System: Power Supply 2 , middle, Not Installed
(FAILED)
Apr 16 18:21:25:A:System: Power Supply 3 , top, Not Installed (FAILED)
Apr 16 18:22:12:I:System: i2c recovered (GIEI = clear), Severity Minor,
Mux index 0, Mux tap 4, ID 0x4, Addr 0x5, (FANTRAY4)
Dynamic Log Buffer (50 lines):
Apr 16 18:22:12:I:System: i2c recovered (GIEI = clear), Severity Minor,
Mux index 0, Mux tap 4, ID 0x4, Addr 0x5, (FANTRAY4)
Apr 16 18:21:27:I:System: bad i2c access (GIEI = set), Severity Minor,
Mux index 0, Mux tap 4, ID 0x4, Addr 0x5, (FANTRAY4)
Apr 16 18:21:25:A:System: bad i2c access (GIEI = set), Severity Major,
Mux index 0, Mux tap 4, ID 0x4, Addr 0x5, (FANTRAY4)
Apr 16 18:21:24:I:System: last good i2c access, Mux index 0, Mux tap 1,
ID 0x9, Addr 0x1, (SNM1TEMP)
```

When the GIEI flag is cleared, the first Syslog message in the static section of the log is updated to show that the GIEI is set to clear. The second Syslog message in the static section is removed. A copy of the updated first Syslog message is also generated in the dynamic section of the log and in SNMP log server.

When a problematic device is removed from the system, the GIEI is cleared and all Syslog messages are updated to show that the GIEI is set to clear.

If an I2C failure has not occurred, there will be no I2C messages in the static log, dynamic log, or SNMP log server. The following example shows output from the **show logging** command when there is no I2C failure.

```
device# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 1 overruns)
Buffer logging: level ACDMEINW, 50 messages logged
level code: A=alert C=critical D=debugging M=emergency E=error
I=informational N=notification W=warning
Static Log Buffer:
Apr 16 18:21:25:A:System: Power Supply 2 , middle, Not Installed (FAILED)
Apr 16 18:21:25:A:System: Power Supply 3 , top, Not Installed (FAILED)
Dynamic Log Buffer (50 lines):
Mar 28 12:36:47:A:System: Set fan speed to MED (75%)
Mar 25 21:40:47:A:System: Set fan speed to MED-HI (90%)
Mar 25 16:30:47:A:System: Set fan speed to MED (75%)
Mar 23 23:12:07:A:System: Set fan speed to MED-HI (90%)
```

If the system detects a major I2C failure, the system prevents the management module from accessing devices through the I2C serial bus. The output from the **show chassis** command and the **show temperature** command reflect this action, as shown in these examples.

```
device# show chassis
*** Note: ***
*** Global I2C Error Indicator is set (severity: Major). ***
*** All I2C access are skipped. ***
*** Extreme MLX-4 device ***
---POWERS ---
Slot Power-On Priority and Power Usage:
Slot2 pri=1 module type=NI-MLX-1Gx20-GC 20-port 10/100/1000 Copper Module power usage=146W
Slot4 pri=1 module type=NI-X-OC48x4 4-port OC48/12 STM16/STM4 Module power usage=132W
---FANS ---
---TEMPERATURE READINGS ---
LP2 Sensor1: 34.500C
LP2 Sensor2: 44.125C
```

The following output is from the **show temperature** command with the GIEI set to major severity.

```
device# show temperature
*** Note: ***
*** Global I2C Error Indicator is set (severity: Major). ***
*** All I2C access are skipped. ***
SLOT #: CARD TYPE: SENSOR # TEMPERATURE (C):
2 LP 1 34.0C
2 LP 2 44.250C
4 LP 1 36.0C
4 LP 2 45.750C
```

Displaying device status and temperature readings

You can display the following information about the router:

- Power-on priority of the device slots
- Status of the fans
- Temperature readings of the management, switch fabric, interface, and fan control modules and the interval at which the system reads the temperature of these modules
- MAC address of the device

To display this information, enter the **show chassis** command at any level of the CLI.

```
device# show chassis
***MLX-4 chassis ***
---POWERS ---
Power 1 (32011000 - AC 1200W): Installed (OK)
Power 2: not present
Power 3: not present
Total power budget for device = 1200 W
Total power used by system core = 183 W
Total power used by LPs = 386 W
Total power available = 631 W
Slot Power-On Priority and Power Usage:
Slot1 pri=1 module type=NI-MLX-1Gx20-GC 20-port 10/100/1000 Copper Module power usage=156W
Slot4 pri=1 module type=NI-X-OC48x8 8-port OC48/12 STM16/STM4 Module power usage=230W
--- FANS ---
right fan tray (fan 1): Status = OK, Speed = MED-HI (90%)
right fan tray (fan 2): Status = OK, Speed = MED-HI (90%)
--- TEMPERATURE READINGS ---
Active Mgmt Module: 36.500C 49.625C
Standby Mgmt Module: 36.250C 51.0C
SNM1: 37.0C
SNM2: 38.0C
SNM3: not present
LP1 Sensor1: 41.5C
LP1 Sensor2: 50.625C
```

```
LP4 Sensor1: 39.0C
LP4 Sensor2: 49.250C
LP4 Sensor3: UNUSED
LP4 Sensor4: 38.5C
LP4 Sensor5: 47.750C
LP4 Sensor6: UNUSED
Fans are in auto mode. Temperature Monitoring Poll Period is 60 seconds
```

The following table describes the **show chassis** command output.

TABLE 38 show chassis command output

Field	Description
Powers	
Power *num* , *part num*	The **Power***num* is the power supply number as positioned in the device. The number of power supplies are as follows: 4-slot devices: 1 - 38-slot devices: 1 - 416-slot devices: 1 - 832-slot devices: 1 - 8 The *part num* is the part number of the power supply purchased. This applies to AC and DC power supplies.
Power *status*	Indicates whether an AC or DC power supply is installed in the specified power supply slot and the status of the power supply, which can be one of the following: • Installed (Shutdown) - The power supply has shut down. A power supply will shut down due to flapping, or if a shut down is enabled manually using the power-off power-supply command. Refer to Enabling a power supply shutdown on page 252. • Installed (OK) - The power supply is functioning properly and supplying power to the device and installed modules. • Failed - The power supply is not functioning and is not supplying power to the device and installed modules. • not present - There is no power supply installed in the slot. • Installed (Failed or Disconnected) - The power supply is not functioning, or the power supply is not connected to the device and installed modules.
Total power budget for device	The sum of all power (in watts), used by all power supplies currently functioning in the device. Refer to Hardware specifications for ExtremeRouting MLX Series routers on page 271.
Total power used by system core	The total power used by the management modules, switch fabric modules, and fans. Each component consumes different amounts of power.
Total power used by LPs	The total power used by the interface modules. Each module type consumes different amounts of power.
Total power available	The total power budget for the device minus the total power used by the system core and the installed interface modules.
Slot Power-On Priority	The configured power-on priority of each interface module.
Slot *num* Slot1 - Slot16 4-slot device: Slot1 - Slot48-slot device: Slot1 - Slot816-slot device: Slot1 - Slot1632-slot device: Slot1 - Slot32	The **slot***num* is the device slot number. The priority of each device slot as configured by the **lp-slot-priority** command. The priority can be 1 (low, default) - 8 (high). If the amount of power supplied to the device falls below a minimum threshold, the device slots with the lowest priority will likely lose power. For information about using the **lp-slot-priority** command, refer to Changing priority of slots for interface modules on page 224.
Fans	
Fan *number*	Information about fans in the device.

TABLE 38 show chassis command output (continued)

Field	Description
Status	The fan status of a fan can be OK or Failed: • OK - The fan is functioning properly and is keeping the temperature of each module within an acceptable range. • Failed - The fan is not working or the fan control module cannot control the fan.
Speed	Fan speed can be one of four settings: • Low - The fan is functioning at 50 percent of capacity. • Medium - The fan is functioning at 75 percent of capacity. • Medium-high - The fan is functioning at 90 percent of capacity. • High - The fan is functioning at 100 percent of capacity.
Temperature readings	
Active and Standby Mgmt Module	The temperature of the active and standby management modules.
Fan *number*	The temperature of fan0 and fan1.
SNM *number*	The temperature of the switch fabric module.
LP *number*	The temperature of the interface module.
Temperature Monitoring Poll Period	The interval at which the system reads the temperature sensor on the management, switch fabric, interface, and fan control modules.
MAC address	
Backplane EEPROM MAC Address	The MAC address of the device.

Displaying the Syslog configuration and static and dynamic buffers

To display the Syslog parameters currently in effect on a device, enter the **show logging** command from any level of the CLI.

```
device> show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Buffer logging: level ACDMEINW, 7 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning
...
```

The following table describes the Syslog output buffer configuration information, in the rows above the log entries.

TABLE 39 Syslog buffer configuration

Field	Description
Syslog logging	The state (enabled or disabled) of the Syslog buffer.
messages dropped	The number of Syslog messages dropped due to user-configured filters. By default, the software logs messages for all Syslog levels. You can disable individual Syslog levels, in which case the software filters out messages at those levels. Each time the software filters out a Syslog message, this counter is incremented.
flushes	The number of times the Syslog buffer has been cleared by the **clear logging** command. For information about clearing the Syslog buffer, refer to Static and dynamic buffers on page 207.
overruns	The number of times the dynamic log buffer has filled up and been cleared to hold new entries. For example, if the buffer is set for 100 entries, the 101st entry causes an overrun. After that, the 201st entry causes a second overrun.

TABLE 39 Syslog buffer configuration (continued)

Field	Description
level	The message levels that are enabled. Each letter represents a message type and is identified by the key (level code) below the value. If you disable logging of a message level, the code for that level is not listed.
messages logged	The total number of messages that have been logged since the software was loaded.
level code	The message levels represented by the one-letter codes.

Static and dynamic buffers

The software provides a static buffer and a dynamic buffer:

- Static - logs power supply failures, fan failures, and temperature warning or shutdown messages
- Dynamic - logs all other message types. In previous releases, power supply messages were displayed in static logs only, with only the last event logged. Beginning with release 03.8.00, power supply messages are displayed in both static and dynamic logs.

In the static log, new messages replace older ones, so only the most recent message is displayed. For example, only the most recent temperature warning message will be present in the log. If multiple temperature warning messages are sent to the log, the latest one replaces the previous one. The static buffer is not configurable.

The message types that appear in the static buffer do not appear in the dynamic buffer. The dynamic buffer contains up to the maximum number of messages configured for the buffer (50 by default), then begins removing the oldest messages (at the bottom of the log) to make room for new ones.

The static and dynamic buffers are both displayed when you enter the **show logging** command.

```
device(config)# show logging
...
Static Log Buffer:
Aug 27 12:42:42:A:Power Supply 6, 1st right, failed
Dynamic Log Buffer (50 lines):
Aug 27 12:19:04:I:Interface ethernet3/4, state up
Aug 27 12:19:04:I:Interface ethernet6/3, state up
Aug 27 12:19:04:I:Interface ethernet3/2, state up
Aug 27 12:19:04:I:Interface ethernet6/1, state up
Aug 27 12:19:00:N:Module up in slot 6
Aug 27 12:19:00:N:Module up in slot 3
Aug 27 12:18:43:I:Warm start
```

When you clear log entries, you can selectively clear the either buffer, or you can clear both. For example, to clear only the dynamic buffer, enter the **clear logging** command at the Privileged EXEC level.

```
device# clear logging dynamic-buffer
```

Syntax: clear logging [**dynamic-buffer** | **static-buffer**]

Specify the **dynamic-buffer** keyword to clear the dynamic buffer, or the **static-buffer** keyword to clear the static buffer. If you do not specify a buffer, both buffers are cleared.

Router Headless State by MP Presence from LP

A router chassis is considered headless on entering a state where the MPs go down. When the chassis enters a router headless state, the LPs are unaware of the MP's state and continue to perform.

When there is a headless router condition, hardware flooding traffic is processed and traffic is dropped that needs to pass through the MP. To avoid this situation, the LP maintains the MP state and brings itself down in case no MPs are present.

To know the presence of MP by LP, accounting of IPC and keep-alive messages from the MP are performed in the LP.

The current state of MP presence is displayed when you enter the **ipc show mp-presence state** CLI command in LP. The command output is as follows:

```
LP-2#ipc show mp-presence state
MP-PRESENCE is in MP_ALIVE
```

The following table lists all the MP-Presence states maintained by LP.

TABLE 40 MP-Presence States for Show MP-Presence State

MP Presence State	
MP_ALIVE	MP_WAIT
MP_SWITCH	MP_ALIVE_DISABLED

By default, MP Presence is enabled. MP presence is toggled when you enter the **ipc toggle mp-presence** CLI command in LP. The command output is as follows:

```
LP-2#ipc toggle mp-presence
IPC MP Presence disabled
LP-2#ipc toggle mp-presence
IPC MP Presence enabled
```

The threshold time is set in the chassis when you enter the command **dm mp-presence-threshold-time** . This command displays a warning message in the LP console before LP is reset after finding the Active MP.

The allowed threshold time is 0 to 35 seconds only. The maximum limit of 35 seconds is maintained because the LP is reset on the MP absence in 35 seconds. The input value 0 clears **mp-presence-threshold-time** .

Commands for setting **mp-presence-threshold** time are shown in the following table.

TABLE 41 Operations for Setting mp-presence-threshold Time

Operation	Result
LP-1#**dm mp-presence-threshold-time 10**	MP Presence threshold time is set to 10 seconds.
LP-1#**dm mp-presence-threshold-time 0**	MP Presence threshold time is cleared.

When LP detects no MPs are present, LP will reset in another 35 seconds. The below warning message is displayed in LP console before reset.

WARNING

```
mp_presence_threshold_log: LP will go for a reset in another 35 seconds.
```

Rolling Reboot

The Rolling Reboot feature provides a solution for continuously rebooting the line card when a system failure occurs from causes including BIST failure, ECC errors, module init failure, and hardware failure during system initialization. When there is failure, the system automatically reboots in an infinite loop until the failure is resolved. Repetitious reboot cycles consume CPU resources, power, and result in unwanted IPC traffic to the MP.

When the system detects the continuous reboot of a line card, that line card is placed into interactive or down state mode after ten (10) consecutive reboot cycles, and a failure message is sent to the MP.

FPGA Image Mismatch

A version mismatch between FPGA applications and hardware results in system failure and continuous reboot on every module initialization failure. The Rolling Reboot feature places the line card into the interactive or down state mode on detection of an FPGA version mismatch.

This feature will detect the incompatibility between application FPGA version and Hardware FPGA version and put the card into down state if there is mismatch.

Monitor/Application Image Mismatch

A version mismatch between the monitor and application image results in system failure. The Rolling Reboot feature places the line card into the interactive or down state mode on detection of a monitor and application image version mismatch.

Line Module Configuration Deletion in Interactive Boot Mode

In this release, line module configurations can be deleted when a module is in Interactive Boot Mode. When an existing LP module is removed from the slot and replaced by an LP module of a different configuration, the LP module boots up to Interactive Boot Mode due to a configuration mismatch. The LP module configuration is not allowed to be removed or updated without manual removal of the LP module.

To avoid physically removing the LP module from the slot and deleting or updating the LP module configuration, the deletion of the LP module configuration is only allowed if the card is in Interactive Boot Mode. The LP module needs a power cycle to return to the Up state. On execution of the "No Module" command, the user is prompted with an option to power cycle the card.

Managing switch fabric modules

This section provides information about how to manage standard switch fabric modules and high speed switch fabric modules.

> NOTE
> In CLI output, standard modules are referred to as generation 1 (G1) modules, and high-speed modules are referred to as generation 2 (G2) modules. The following interface modules are classified by the system as G2 modules: 8x10G, 100G modules. All other interface modules such as 4-port 10G, 2-port 10G, 20-port 1G, 24-port 1G, and 48-port 1G modules are classified by the system as G1 modules.

High speed switch fabric (HSF) modules can operate in Normal mode or Turbo mode. Standard switch fabric modules (SFM) can only operate in Normal mode. The HSF module is classified as a G2 module and SFM module is classified as a G1 module.

When operating in Normal mode, the system uses fixed size cells across the backplane. When operating in Turbo mode, the system uses variable size cells across the backplane. Turbo mode provides higher performance since it is a more efficient mechanism of sending cells across the backplane.

The system selects the operating mode for switch fabric modules at startup, or when the first switch fabric or interface module is installed. The system uses this mode for all modules that are subsequently installed. HSF modules will boot in Turbo mode only if all active interface modules are G2 modules. In a chassis loaded with G1 and G2 modules, the HSF modules will default to Normal mode.

> NOTE
> If a system is operating in Turbo mode, G1 interface modules are blocked from operation. The user has to change the switch fabric mode to Normal mode and restart the system before using the G1 interface modules.

If the system fabric mode is changed to Normal mode from Turbo mode, or vice versa, the system will not change the current operating mode unless the chassis is reloaded.

NOTE
Changes to the switch fabric operating mode do not take effect until after a system reload.

The switch fabric modes have the following restrictions:

- The system blocks discovery of any standard switch fabric (G1) module if you have issued the **system-init block-g1-sfm** command. Refer to Blocking discovery of G1 switch fabric modules on page 210.
- If the system is operating in Turbo mode, standard switch fabric modules (G1) and standard (G1) interface modules are automatically blocked.
- If there are any active G1 switch fabric modules, G2 interface modules are blocked.
- If there are any active G2 interface modules, G1 switch fabric modules are blocked.

Forcing HSF modules to operate in normal mode

NOTE
This procedure requires that you restart your router.

If necessary, you can configure HSF modules to operate in normal mode using the **system-init fabric-data-mode force normal** command.

```
device(config)# system-init fabric-data-mode force-normal
```

If you remove the forced normal condition using the **no** version of this command, you must enter the **write-memory** command and restart the router.

NOTE
4x40G normal mode does not support line rate traffic for smaller packet sizes (64-200B).

Blocking discovery of G1 switch fabric modules

NOTE
This procedure requires that you restart your router.

In a router with both standard (G1) switch fabric modules and G2 HSF modules, you can block the discovery of the G1 switch fabric modules by entering the **system-init block-g1-sfm** command.

After you enter this command, enter the **write -memory** command and restart the router.

Managing the cooling system

This section provides configuration, management, and monitoring information about router cooling systems.

Configuring the cooling system

Your router is pre-configured with default settings for all cooling system parameters. Although no initial configuration of the cooling system is necessary, you can change the settings of the following cooling system parameters:

- Low and high temperature thresholds for modules and fan speeds

- Interval at which the system polls the temperature sensors on the module for a reading

  NOTE
  Auto control of fan speed is not monitored when cards are in interactive mode. Set fan speed to high to prevent over-temp condition.

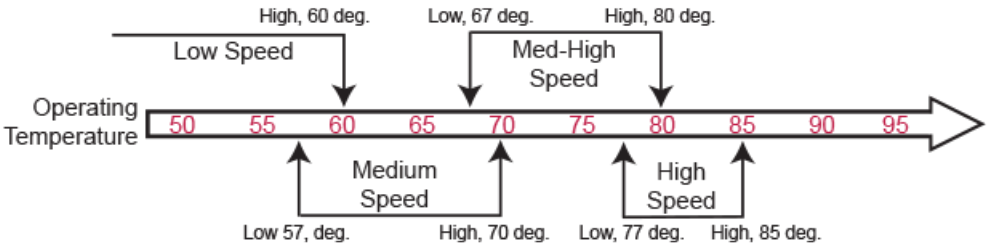
  NOTE
  Adjusting fan controls out of the default setting can negatively affect the efficient cooling of blades and may cause a blade to overheat and shutdown.

Changing temperature thresholds for modules and fan speeds

The cooling system includes fans that operate at four speeds: low, medium, medium-high, and high. In general, each fan speed, (except for low), has a low and high temperature threshold associated with it, as shown in the following figure. The low fan speed has a high temperature threshold only.

NOTE
Adjusting fan controls out of the default setting can negatively affect the efficient cooling of blades and may cause a blade to overheat and shutdown.

FIGURE 107 Fan speeds and temperature thresholds



The low and high temperature thresholds allow the router to determine the speed at which the fans should operate. In general, the fans operate according to these guidelines:

- If the temperature of all modules falls between the low and high thresholds for a fan speed, the fan continues to operate at that speed.
- If the temperature of a management module, switch fabric module, or one interface module exceeds the high threshold specified for a fan speed, the fan changes to the next higher speed. If the temperature of any of the modules exceeds the high threshold for the high speed, the router shuts down the modules to prevent damage. The router also sends a warning message to the system log and an SNMP trap. For information about viewing the warning messages, refer to Displaying temperature warnings on page 218.
- The frequency with which the temperature is checked is determined by the setting of the **temp-poll-period** command. For information about **temp-poll-period** command, refer to Changing the temperature polling interval on page 216.
- If the temperature of a management module, switch fabric module, and interface modules falls below the low threshold for a fan speed, the fan changes to the next lower speed. If the temperature of all modules falls below the high threshold for the low speed, the fan operates at the low speed.

Default temperature thresholds for the MLX Seriesdevices are described in the following table.

TABLE 42 Default temperature thresholds for modules and fan speeds for MLX Series devices

Fan speed	Low temperature threshold	High temperature threshold
Management modules		
High	72 ° C	85 ° C
Medium-high	67 ° C	80 ° C
Medium	52 ° C	70 ° C
Low	-1 °	60 ° C
Management modules CPU		
High	72 ° C	95 ° C
Medium-high	65 ° C	80 ° C
Medium	63 ° C	74 ° C
Low	-1 °	70 ° C
Interface modules		
High	65 ° C	95 ° C
Medium-high	63 ° C	81 ° C
Medium	61 ° C	79 ° C
Low	-1 °	74 ° C
Interface modules Packet Processor		
High	77 ° C	113 ° C
Medium-high	72 ° C	94 ° C
Medium	69 ° C	92 ° C
Low	-1 °	90 ° C
Generation 2 Interface modules		
High	70 ° C	95 ° C
Medium-high	62 ° C	80 ° C
Medium	58 ° C	75 ° C
Low	-1 °	70 ° C
Generation 2 Interface modules Packet Processor		
High	74 ° C	113 ° C
Medium-high	70 ° C	87 ° C
Medium	66 ° C	85 ° C
Low	-1 °	83 ° C
Switch fabric module		
High	47 ° C	75 ° C
Medium-high	37 ° C	50 ° C
Medium	27 ° C	40 ° C
Low	-1 °	30 ° C
High-Speed Switch fabric module		
High	6 2° C	1 00° C
Medium-high	57 ° C	70 ° C
Medium	5 3° C	6 5° C
Low	-1 °	60 ° C

For information about checking the current low and high temperature threshold settings for modules and fan speeds, refer to Displaying temperature thresholds for modules and fan speeds on page 213.

> **NOTE**
> Adjusting fan controls out of the default setting can negatively affect the efficient cooling of blades and may cause a blade to overheat and shutdown.

You can change the default low and high temperature thresholds for a particular module and fan speed. For example, to change the low and high thresholds of the medium fan speed for the management modules to 56 ° C and 72 ° s C, respectively, enter the following command at the global CONFIG level of the CLI.

```
device(config)# fan-threshold mp med 56 72
```

Syntax: fan-threshold | *module*[**low***high-threshold*] [**med***low-threshold high-threshold*][**med-hi***low-threshold high-threshold*][**high***low-threshold high-threshold*]

For the *module* parameter, you can specify the following:

- lp - Changes low and high temperature thresholds for Gen 1 interface modules
- lp2 - Changes low and high temperature thresholds for Gen 2 interface modules
- mp - Changes low and high temperature thresholds for management modules
- mp-cpu - Changes low and high temperature thresholds for the management module CPU
- switch-fabric - Changes low and high temperature thresholds for non-high-speed switch fabric modules
- switch-fabric-g2 - Changes low and high temperature thresholds for high speed switch fabric modules (hSFM)

For the *low-threshold* and *high-threshold* parameters, you can specify any temperature in Centigrade. However, when changing low and high temperature thresholds for module fan speeds, remember that the low temperature threshold of a higher fan speed must be lower than the high temperature threshold of the lower fan speed. Extreme Networks has established this guideline to ensure fan speed stability.

For example, if you are changing the temperature thresholds for a management module high and medium-high fan speeds, the system will accept the following values because the low temperature threshold for the high speed (79 ° C) is lower than the high temperature threshold (82 ° C) for the medium-high speed.

Fan speed	Low temperature threshold	High temperature threshold
High	79 ° C	87 ° C
Medium-high	69 ° C	82 ° C

The device will not accept the following values because the low temperature threshold for the high speed (83 ° C) is higher than the high temperature threshold (82 ° C) for the medium-high speed.

Fan speed	Low temperature threshold	High temperature threshold
High	83 ° C	87 ° C
Medium-high	69 ° C	82 ° C

Displaying temperature thresholds for modules and fan speeds

To check the current settings of the low and high temperature thresholds for modules and fan speeds, you can enter the **show fan-threshold** command at any level of the CLI.

```
device# show fan-threshold
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_MP) ===
```

```
Fan Speed Low: -1 - 60
Fan Speed Med: 57 - 70
Fan Speed Med-Hi: 67 - 80
Fan Speed Hi: 77 - 85
state = 0 (FAN_STATE_LOW)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_SNM) ===
Fan Speed Low: -1 - 30
Fan Speed Med: 27 - 40
Fan Speed Med-Hi: 37 - 50
Fan Speed Hi: 47 - 75
state = 2 (FAN_STATE_MED_HI)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_LP) ===
Fan Speed Low: -1 - 50
Fan Speed Med: 46 - 55
Fan Speed Med-Hi: 51 - 60
Fan Speed Hi: 56 - 95
state = 0 (FAN_STATE_LOW)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_LP_XPP) ===
Fan Speed Low: -1 - 50
Fan Speed Med: 45 - 65
Fan Speed Med-Hi: 60 - 75
Fan Speed Hi: 70 - 113
state = 1 (FAN_STATE_MED)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_STANDBY_MP) ===
Fan Speed Low: -1 - 60
Fan Speed Med: 57 - 70
Fan Speed Med-Hi: 67 - 80
Fan Speed Hi: 77 - 85
state = 0 (FAN_STATE_LOW)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_MP_CPU) ===
Fan Speed Low: -1 - 60
Fan Speed Med: 57 - 70
Fan Speed Med-Hi: 67 - 80
Fan Speed Hi: 77 - 95
state = 1 (FAN_STATE_MED)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
=== Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_STANDBY_MP_CPU) ===
Fan Speed Low: -1 - 60
Fan Speed Med: 57 - 70
Fan Speed Med-Hi: 67 - 80
Fan Speed Hi: 77 - 95
state = 0 (FAN_STATE_LOW)
max_ts_shut_off_count = 1
shut_off_count = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

The output displays the following information.

TABLE 43 Temperature threshold information for modules and fan speeds

This field...	Displays...
Thermal Sensor Control Block (THERMAL_SENSOR_TEST_RULE_module)	The temperature threshold information for the various modules. The *module* parameter indicates the following: • MP - The active management module • STANDBY_MP - The standby management module • SNM - The switch fabric module • LP - An interface module

TABLE 43 Temperature threshold information for modules and fan speeds (continued)

This field...	Displays...
Fan Speed Low or Med or Med-Hi or Hi	The current setting of the low and high temperature thresholds for the low, medium, medium-high, and high fan speeds. NOTE As indicated in Table 44, the low fan speed for each module does not have a default low temperature threshold value, nor can you configure this value. The "-1" value that appears in the Fan Speed Low field for each module is a Extreme internal value only.
State = 0 (FAN_STATE_LOW)	For Extreme internal use only.
max_ts_shut_off_count	For Extreme internal use only.
shut_off_count = 0 0 0 0 0 0 0 0	For Extreme internal use only.

When syslog messages display a change in fan speed, you can identify which sensors triggered the change by checking **show chassis** and **show fan-threshold** command output and looking for sensors with temperatures near threshold boundaries. The following table lists the associations between the **show chassis** , **show fan-threshold** , and **fan-threshold commands** .

NOTE
A "thermal block" refers to the group of high and low thresholds for all fan speed levels.

TABLE 44 Associations between show chassis, show fan threshold, and fan-threshold commands

show chassis command output (sensors)	**show fan-threshold** command output (thermal block)	**fan-threshold** command configuration
MP, SFM, and hSFM Modules		
Active Management 1st reading	THERMAL_SENSOR_TEST_RULE_MP	fan-threshold mp
Active Management 2nd reading	THERMAL_SENSOR_TEST_RULE_MP_CPU	fan-threshold mp-cpu
Standby Management 1st reading	THERMAL_SENSOR_TEST_RULE_STANDBY_MP	fan-threshold mp
Standby Management 2nd reading	THERMAL_SENSOR_TEST_RULE_STANDBY_MP_CPU	fan-threshold mp-cpu
SFM FE1 reading	THERMAL_SENSOR_TEST_RULE_SNM	fan-threshold switch-fabric
SFM FE2 reading	THERMAL_SENSOR_TEST_RULE_SNM	fan-threshold switch-fabric
SFM FE3 reading	THERMAL_SENSOR_TEST_RULE_SNM	fan-threshold switch-fabric
hSFM FE1 reading	THERMAL_SENSOR_TEST_RULE_SNM_G2	fan-threshold switch-fabric-g2
hSFM FE2 reading	THERMAL_SENSOR_TEST_RULE_SNM_G2	fan-threshold switch-fabric-g2
hSFM FE3 reading	THERMAL_SENSOR_TEST_RULE_SNM_G2	fan-threshold switch-fabric-g2
LP Modules (1 or 2 Traffic Managers)		
LP Sensor 1 reading (TM 0)	THERMAL_SENSOR_TEST_RULE_LP	fan-threshold lp
LP Sensor 2 reading (TM 0)	THERMAL_SENSOR_TEST_RULE_LP_XPP	N/A (Must not be changed)
LP Sensor 3 reading (TM 1)	THERMAL_SENSOR_TEST_RULE_LP	fan-threshold lp
LP Sensor 4 reading (TM 1)	THERMAL_SENSOR_TEST_RULE_LP_XPP	N/A (Must not be changed)
NI-MLX-10Gx8-M LP Modules		
LP2 Sensor 1 reading	THERMAL_SENSOR_TEST_RULE_LP_2	fan-threshold lp2
LP2 Sensor 2 reading	THERMAL_SENSOR_TEST_RULE_LP_XPP2	N/A (Must not be changed)
LP2 Sensor 3 reading	UNUSED	UNUSED
LP2 Sensor 4 reading	THERMAL_SENSOR_TEST_RULE_LP_2	fan-threshold lp2

TABLE 44 Associations between show chassis, show fan threshold, and fan-threshold commands (continued)

show chassis command output (sensors)	**show fan-threshold** command output (thermal block)	**fan-threshold** command configuration
LP2 Sensor 5 reading	THERMAL_SENSOR_TEST_RULE_LP_XPP2	N/A (Must not be changed)
LP2 Sensor 6 reading	UNUSED	UNUSED
LP2 Sensor 7 reading	UNUSED	UNUSED
BR-MLX-100Gx2-X LP Modules		
LP2 Sensor 1 reading	THERMAL_SENSOR_TEST_RULE_LP_2	fan-threshold lp2
LP2 Sensor 2 reading	THERMAL_SENSOR_TEST_RULE_LP_XPP2	N/A (Must not be changed)
LP2 Sensor 3 reading	UNUSED	UNUSED
LP2 Sensor 4 reading	THERMAL_SENSOR_TEST_RULE_LP_2	fan-threshold lp2
LP2 Sensor 5 reading	THERMAL_SENSOR_TEST_RULE_LP_XPP2	N/A (Must not be changed)
LP2 Sensor 6 reading	UNUSED	UNUSED
LP2 Sensor 7 reading	UNUSED	UNUSED
LP2 Sensor 8 reading	UNUSED	UNUSED
LP2 Sensor 9 reading	UNUSED	UNUSED
LP2 Sensor 10 reading	UNUSED	UNUSED
LP2 Sensor 11 reading	UNUSED	UNUSED
LP2 Sensor 12 reading	UNUSED	UNUSED

Changing the temperature polling interval

By default, the router reads the temperature sensor on each module every 60 seconds. To change the polling interval, enter the **temp-poll-period** command at the global CONFIG level of the CLI.

```
device(config)# temp-poll-period 120
```

Syntax: temp poll period log threshold *seconds*

For the *seconds* parameter, you can specify a value from 30 - 120.

> NOTE
> Adjusting temperature polling interval out of the default setting can negatively affect the efficient cooling of blades and may cause a blade to overheat and shutdown.

Manually setting the fan speed

Typically, the management module, in conjunction with default settings of low and high temperature thresholds, determines the speed of the two four-speed fans. (For information about changing the low and high temperature thresholds, refer to Changing temperature thresholds for modules and fan speeds on page 211.) You can manually set the fan speed using the **set-fan-speed** command in the Global CONFIG level of the CLI.

> NOTE
> Auto control of fan speed is not monitored when cards are in interactive mode. Set fan speed to high to prevent over-temp condition.

> NOTE
> Setting a value other than auto or high disables auto fan control and will negatively affect the efficient cooling of blades and may cause a blade to overheat and shutdown.

For example, to set the speed of fan 0 to medium-high, enter the following command.

```
device# set-fan-speed med-high
```

For the *fan-speed* parameter, you can specify the following:

Syntax: set fan speed [**auto** | **high** |**low** |**med** | **med-high**]

- auto - The system is adjusted by the monitoring system.
- high - The system sets the fan speed to high.
- low - The system sets the fan speed to low.
- med - The system sets the fan speed to medium.
- med-high - The system sets the fan speed to medium-high.

Monitoring the cooling system

You can monitor the following aspects of the router cooling system:

- The temperature of the fan control modules
- The status and speed of the fans
- The temperature warnings sent to the system log and that generate an SNMP trap

Displaying fan tray status and speed

To display the status and speed of the 4-speed fans in the router, enter the **show chassis** command at any level of the CLI.

```
device# show chassis
...
--- FANS ---
Back fan tray 1: Status = OK, Speed = LOW (50%)
Back fan tray 2: Status = OK, Speed = LOW (50%)
Back fan tray 3: Status = OK, Speed = LOW (50%)
Back fan tray 4: Status = OK, Speed = LOW (50%)
```

For information about all output generated by the **show chassis** command, refer to Displaying device status and temperature readings on page 204.

TABLE 45 Fan status and speed fields

Field	Description
Status	The status can be one of the following: • OK - The fan is functioning properly and is keeping the temperature of each module within an acceptable temperature range. • Failed - The fan is not functioning properly or the fan control module cannot control the fan.
Speed	The speed can be one of the following: • LOW - The fan is functioning at 50 percent of capacity. • MEDIUM - The fan is functioning at 75 percent of capacity. • MEDIUM-HIGH - The fan is functioning at 90 percent of capacity. • HIGH - The fan is functioning at 100 percent of capacity.

Displaying temperature warnings

If the temperature of a module exceeds the high temperature threshold for any of the fan speeds, the system sends a warning message to the system log and an SNMP trap. (For more information about the low and high temperature thresholds, refer to Changing temperature thresholds for modules and fan speeds on page 211.) This section describes how to view the system log. If you have configured your router to use a Syslog server or SNMP trap receiver, refer to the documentation for the server or receiver.

To display the system log, enter the show log command at any CLI level.

```
device# show log
```

Temperature log reduction

Depending on settings and temperature readings, fan speeds are changed dynamically within the following ranges: low, med, med-hi, and high. Fan speed changes are determined by temperature thresholds set for sensors on the management modules, interface modules and switch fabric modules. When a temperature threshold is passed upward on any module, the fan speed changes to the assigned fan speed. This occurs even if the temperature is within the threshold for the slower fan speed on other modules. In previous versions of the software, a log message is sent whenever a temperature threshold is crossed on any module whether the fan speed is actually increased or not. This can result in excessive log messages.

The default behavior is a for log message to be sent only when the fan speed is actually changed, which reduces the number of messages. A CLI option allows you to log all messages or have a single log message sent when any temperature threshold is crossed.

Details about how to set temperature thresholds and default threshold values are described in the Configuring the cooling system on page 210

Configuring temperature logging

The **temp log-threshold** command sets the temperature logging threshold to send a single message whenever any of the thresholds are crossed.

```
device(config) temp-log-threshold low
```

Syntax: temp log threshold [**verbose** | **high** |**low** |**med** | **med-high**]

- The *verbose* option generates logs whenever a temperature threshold is crossed. This is the operational mode of previous versions of Multi-Service IronWare software and provides backward compatibility.
- The *high* option generates logs only when the high threshold is crossed.
- The *low* option generates logs whenever any threshold (low, medium, medium-high or high) is crossed.
- The *med* option generates logs only when the medium, medium-high, and high thresholds are crossed.
- The *med-high* option generates logs only when the medium-high and high thresholds are crossed. This is the default setting.

This output displays two instances of a module temperature exceeding the warning threshold.

Managing interface modules

Configuring interface module boot parameters

Ethernet interface modules contain independent copies of system software and boot after the management module boots. By default, the following boot-related events occur:

- The router synchronizes, or prompts you to synchronize, the software image on the interface modules with the software on the management module.
- Interface modules boot from a source specified by the management module (the default source is a primary image in the flash memory on the interface module.)

You can make these changes:

- Disable the synchronization of images between the management module and all interface modules. You can also initiate an immediate synchronization.
- Change the boot source of one or all interface modules.

Synchronizing the software image between management modules and interface modules

An interface module can have primary and secondary images that reside in the flash memory.

If you copy the primary or secondary image to all interface modules using the **copy** command with the **all** keyword, the management module makes a copy of the file and stores it in code flash under the names **lp-primary-0** or **lp-secondary-0** . The images are stored in this location only and are not run by the management module or the interface modules. If you copy the primary or secondary image to a specified device slot using the **copy** command with the *device-slot-number* parameter, the management module does not make a copy of the file.

If the management module has a copy of the primary or secondary image in code flash, by default, the router synchronizes, or prompts you to synchronize, images between the management module and the interface modules during the boot process. When the router synchronizes the images, the management module copies the images from flash memory to the flash memory on the interface module (the default boot source for the interface modules).

You can manage synchronization of the software images between management and interface modules in the following situations:

- You are prompted to synchronize the software images during the boot process.
- You want to initiate an immediate synchronization; for example, you want an immediate update of the software images on one or all interface modules.
- You want to disable synchronization; for example, you have upgraded the image of one interface module but want to continue running the older image on all other interface modules.

The following sections discuss how to manage software image synchronization in these situations.

Synchronizing the software image on interface modules during the boot process

By default, the router checks the software images in the flash memory on interface modules during the boot process to see if they are the same as the images in the flash memory on the management module. If an interface module does not have a software image, the system automatically downloads the image from the management module to the interface module.

If an interface module has an image that is different from that on the management module, the system prompts you to take one of the following steps:

- To update the primary and secondary images on the interface module with the images on the management module, enter the **lp cont-boot sync***slot-number* command at the Privileged EXEC prompt.
- To retain the software images on the interface module, enter the **lp cont-boot no-sync***slot-number* command at the Privileged EXEC prompt.

Syntax: lp cont boot sync *slot-number*

Syntax: lp cont boot no sync *slot-number*

Specifying an immediate synchronization

To immediately synchronize software images between the management module and one or all interface modules, enter the following command at the Privileged EXEC level.

```
device# lp sync all
```

Syntax: lp sync [**all**|*slot-number*]

- The **all** keyword indicates that the immediate synchronization applies to all interface modules in the router.
- The *slot-number* parameter specifies the slot number that contains the interface module to which the immediate synchronization applies. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Specifying an immediate shutdown

The management module takes approximately 16-20 seconds to shutdown all interface modules in a device after a reload is issued. During this time, the interface module continues sending packets. Enter the **lp fast-powerdown** command to immediately shut down all interface modules in a device after a reload is issued.

```
device(config)# lp fast-powerdown
```

If you do not enter this command, by default, the interface module continues to forward packets for an extended time after the router is reloaded.

> NOTE
> You do not need to change the state of the interface module, or synchronize this shutdown with the standby management module.

Changing the boot source

By default, the interface modules boot from the primary image located in flash memory. You can change the boot source of one or all interface modules to one of the following sources:

- Management module
  - auxiliary flash card in slot 1 or 2
  - Primary or secondary image in the management module flash memory
- Interface module
  - Secondary image in interface module flash memory
- TFTP server

You can also specify an interactive boot, which allows you to enter a separate command after the interface module comes up. The command specifies the source from which one or all interface modules should boot.

When changing the boot source for one or all interface modules, you can specify one of the following:

- An immediate boot for one interface module from a specified source
- An automatic boot for one or all interface modules from a specified source starting with the next software reload or system reset and each reload or reset after that

The CLI command for specifying an immediate boot for one interface module is the same as that for specifying an automatic boot for one or all modules. The only difference is the CLI level from which you execute the command. You must specify the command for an immediate boot in the Privileged EXEC level and the command for an automatic boot in the global CONFIG level.

The following sections explain how to specify an immediate boot and an automatic boot.

Specifying an immediate boot

You can specify an immediate boot for one interface module from a specified source by entering the **lp boot system** command in the Privileged EXEC level. The entered command will override the default or configured boot source one time only.

Specifying an immediate boot from the auxiliary flash slots on the management module

To specify an immediate boot for the interface module installed in slot 1 from the auxiliary flash slot on the management module, enter the **lp boot system** command at the Privileged EXEC level of the CLI.

```
device# lp boot system slot1 primary 1
```

Syntax: lp boot system [**slot1** | **slot2**] *filename slot-number*

- The **slot1** and **slot2** keywords indicate the auxiliary flash slot on the management module from which to boot the interface module.
- The *filename* parameter specifies the name of the image from which to boot the interface module.
- The *slot-number* parameter specifies the device slot number that contains the interface module that will undergo an immediate boot. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Specifying an immediate boot from management module flash memory

To specify an immediate boot from the primary image on the management module for the interface module installed in slot 1, enter the following command at the Privileged EXEC level of the CLI.

```
device# lp boot system mp primary 1
```

Syntax: lp boot system mp [**primary** | **secondary**] *slot-number*

- The **primary** and **secondary** keywords specify the primary or secondary software image in flash memory on the management module.
- The *slot-number* parameter specifies the device slot number that contains the interface module that will undergo an immediate boot.You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Specifying an immediate boot from flash memory on the interface module

To specify an immediate boot from the primary image in flash memory on the interface module installed in slot 1, enter the following command at the Privileged EXEC level of the CLI.

```
device# lp boot system flash primary 1
```

Syntax: lp boot system flash [**primary** | **secondary**] *slot-number*

- The **primary** and **secondary** keywords specify the primary or secondary image in the interface module flash memory.

- The *slot-number* parameter specifies the slot number that contains the interface module that will undergo an immediate boot.You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Specifying an immediate boot from a TFTP server

To specify an immediate boot for the interface module installed in slot 1 from a TFTP server, enter the following command at the Privileged EXEC level of the CLI.

```
device# lp boot system tftp 123.123.123.123 primary 1
```

Syntax: lp boot system tftp *ip-addressfilenameslot-number*

- The *ip-address* parameter specifies the IP address of the TFTP server from which the interface module will be booted.
- The *filename* parameter specifies the name of the image from which to boot the interface module.
- The *slot-number* parameter specifies the slot number that contains the interface module that will undergo an immediate boot. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Specifying an immediate interactive boot

To specify an immediate interactive boot for the interface module installed in slot 1, enter the following command at the Privileged EXEC level of the CLI.

```
device# lp boot system interactive 1
```

Syntax: lp boot system interactive *slot-number*

- The *slot-number* parameter specifies the slot number that contains the interface module that will undergo an immediate boot. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

After you enter this command, the system enters monitor mode on the interface module. To boot from the primary image in flash memory on the interface module, enter the following command at the monitor prompt.

```
LP MONITOR> boot system flash primary
```

Configuring an automatic boot

To configure an automatic boot for one or all interface modules from a specified source, enter the **lp boot system** command in the global CONFIG level. If you save this configuration by entering the **write memory** command, the system implements the automatic boot starting with the next software reload or system reset and each reload or reset after that.

Configuring an automatic boot from the auxiliary flash slot on the management module

To configure an automatic boot for all interface modules from auxiliary flash slot1 on the management module, enter the following command at the global CONFIG level of the CLI.

```
device(config)# lp boot system slot1 primary all
```

Syntax: lp boot system [**slot1** | **slot2**] *filename* [**all** | *slot-number*]

- The **slot1** and **slot2** keywords indicate the auxiliary flash slot on the management module from which to boot the interface modules.
- The *filename* parameter specifies the name of the image from which to boot the interface modules.

- The **all** | *slot-number* parameter specifies that the automatic boot applies to all interface modules in the device or to an interface module in the specified device slot number only. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Configuring an automatic boot from flash memory on the management module

To configure an automatic boot from the primary image in flash memory on the management module for all interface modules, enter the following command at the global CONFIG level of the CLI.

```
device(config)# lp boot system mp primary all
```

Syntax: lp boot system mp [**primary** | **secondary**] [**all** | *slot-number*]

- The **primary** and **secondary** keywords specify the primary or secondary image in flash memory on the management module.
- The **all** | *slot-number* parameter specifies that the automatic boot applies to all interface modules in the device, or to an interface module in the specified device slot number only. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Configuring an automatic boot from flash memory on the interface module

To configure an automatic boot from the primary image in flash memory on the interface module for all interface modules, enter the following command at the global CONFIG level of the CLI.

```
device(config)# lp boot system flash primary all
```

Syntax: lp boot system flash [**primary** | **secondary**] [**all** | *slot-number*]

- The **primary** and **secondary** keywords specify the primary or secondary image in the interface module flash memory.
- The **all** | *slot-number* parameter specifies that the automatic boot applies to all interface modules in the device or to an interface module in the specified slot number only. You can specify 1 - 4 for 4-slot devices, 1 - 8 for 8-slot devices, 1 - 16 for 16-slot devices, or 1 - 32 for 32-slot devices.

Configuring an automatic boot from a TFTP server

To configure an automatic boot for all interface modules from a TFTP server, enter the following command at the global CONFIG level of the CLI.

```
device(config)# lp boot system tftp 123.123.123.123 primary all
```

Syntax: lp boot system tftp *ip-addressfilename* [**all** | *slot-number*]

- The *ip-address* parameter specifies the IP address of the TFTP server from which the interface modules will be booted.
- The *filename* parameter specifies the name of the image from which to boot the interface modules.
- The **all** | *slot-number* parameter specifies that the automatic boot applies to all interface modules in the router or to an interface module in the specified router slot number. You can specify 1 - 4 for 4-slot routers, 1 - 8 for 8-slot routers, 1 - 16 for 16-slot routers, or 1 - 32 for 32-slot routers.

Configuring an automatic interactive boot

To configure an automatic interactive boot for all interface modules, enter the following command at the global CONFIG level of the CLI.

```
device(config)# lp boot system interactive all
```

Syntax: lp boot system interactive [**all** | *slot-number*]

The **all** | *slot-number* parameter specifies that the automatic boot applies to all interface modules in the router, or to an interface module in the specified slot number. You can specify 1 - 4 for 4-slot routers, 1 - 8 for 8-slot routers, 1 - 16 for 16-slot routers, or 1 - 32 for 32-slot routers.

After you enter this command, the system enters monitor mode on the interface module. To boot from the primary image in flash memory on the interface module, enter the following command at the monitor prompt.

```
LP MONITOR> boot system flash primary
```

Syntax: boot system flash primary

Changing priority of slots for interface modules

You can prioritize the slots in which the interface modules are installed. The priority range is 1 (low) - 8 (high). You can set one, some, or all slots to the same priority or each slot to a different priority. If you assign the same priority to all slots, the lowest-number slot has the highest priority, while the highest-numbered slot has the lowest priority.

By default, the priority of all slots is 1, which is the lowest priority. If the supply of power to the router falls below a minimum threshold, the slots will likely lose power because of their low priority. In this scenario for an 8-slot router, slot 8 will lose power first, then slot 7, slot 6, and so on until slot 1 loses power.

To set the priority of slot 1 to the highest priority (8), enter the following command.

```
device(config)# lp-slot-priority 1 8
```

Syntax: lp-slot-priority *slot-numberpriority*

- The *slot-number* parameter indicates that the slot number for which you are changing the priority. You can specify 1 - 4 for 4-slot routers, 1 - 8 for 8-slot routers, 1 - 16 for 16-slot routers, or 1 - 32 for 32-slot routers.
- The *priority* parameter indicates the priority of the slot if the router loses power. You can specify a value of 1 - 8, where 1 is the lowest priority and 8 is the highest priority. You can set one, some, or all slots to the same priority or each slot to a different priority.

Disabling and re-enabling power to interface modules

You can disable and re-enable power to a specified interface module, or to all interface modules. For example. to disable power to the interface module in slot 1, enter the following command at the Privileged EXEC level of the CLI.

```
device# power-off lp 1
```

To disable power on all interface modules, enter the following command:

```
device# power-off lp all
```

In this output example, there is one interface module in slot 2, which is powered off.

```
device# power-off lp all
Slot 2 is powered off.
rw_power_off_lp: write 00030000 to RW_MBRIDGE_CARD_POWER_OFF_REG
```

Syntax: power-off lp *slot-number* **all**

- The *slot-number* parameter indicates the slot number for which you are disabling the power. You can specify 1 - 4 for 4-slot routers, 1 - 8 for 8-slot routers, 1 - 16 for 16-slot routers, or 1 - 32 for 32-slot routers.
- The **all** parameter allows you to power off all interface modules.

To re-enable power to the interface module in slot 1, enter the following command at the Privileged EXEC level of the CLI.

```
device# power-on lp 1
```

To re-enable power on all interface modules, enter the following command.

```
device# power-on lp all
```

In this output example, there is one interface module in slot 3 and slot 3 is powered on.

```
device# power-on lp all
Slot 3 is powering on.
rw_power_on_lp: write 00070004 to RW_MBRIDGE_CARD_POWER_OFF_REG
```

Syntax: power-on lp [*slot-number* | **all**]

- The *slot-number* parameter indicates the slot number for which you are re-enabling the power. You can specify 1 - 4 for 4-slot routers, 1 - 8 for 8-slot routers, 1 - 16 for 16-slot routers, or 1 - 32 for 32-slot routers.
- The **all** parameter allows you to power on all interface modules.

Monitoring Link Status

Software and hardware error conditions can bring down fabric links. When all links connecting a traffic manager to a backplane are down, the traffic manager will drop incoming traffic. If the port is still up, the traffic manager will continue to drop data. Extreme NetIron software R05.3.00 and later solved this problem by continuously running a software task on the LP that monitors link status. If it detects that the fabric links between the traffic manager and the backplane are down, the software shuts down the ports connected to that traffic manager, resulting in no continuous traffic drop. If all of the following criteria are met, the software brings the ports back up:

- all the links come back up
- at least 30 percent of the total links are in the "up" state
- the port is enabled and there are no additional blocking conditions

Enabling monitoring link status

This feature is included by default in the Extreme NetIron software R05.3.00 and later; no configuration is required to enable it.

Disabling monitoring link status

To disable the link status monitoring feature, enter the following command:

```
no system-monitoring tm port-control
```

Displaying fabric link status

To display the fabric link status, enter the following command:

```
MLX#show sfm-links 1
 SFM#/FE# | FE link#  | LP#/TM# | TM link#  | link state
----------+-----------+---------+-----------+---------
  1 / 1   |    13     | 2 / 1   |    13     |      UP
  1 / 1   |    17     | 2 / 2   |    01     |      DOWN
  1 / 1   |    14     | 2 / 1   |    01     |      UP
```

Syntax: show sfm-links *sfm-number* | **all** [**errors**]

The *sfm-number* variable specifies an SFM that you want to display link information for.

The **all** option displays link information for all SFMs in the chassis.

The *errors* option only displays information for SFM links that are in the DOWN state.

The output of this command can also be filtered using an output modifier. To use an output modifier, type a vertical bar (|) followed by a space and one of the following parameters:

- *begin* - begin output with the first matching line
- *exclude* - exclude matching lines from the output
- *include* - include only matching lines in the output

A warning statement is sent if the number of operational links falls below the minimum threshold.

This warning is displayed to warn users that the line rate traffic will not be maintained.

The following table describes the information the **show sfm-links** command displays.

TABLE 46 CLI display of SFM link information

This field...	Displays...
SFM#	The switch fabric module number.
FE#	The FE number.
FE link#	The number of the interconnect between the SFM and the FE.
LP#	The slot number where the Interface module (LP) is installed.
TM#	The number of the traffic manager used in the link.
TM link#	The link number on the traffic manager.
link state	The link state is either: UP - In an operating condition DOWN - In a non-operational condition

Syslog messages

The following syslog messages are related to link monitoring:

- System: Interface Ethernet 3/1, state down -fabric connectivity down
- System: Interface Ethernet 3/1, state up -fabric connectivity up

Traffic Manager XPP link monitoring

Traffic Manager (TM) XPP link status is checked during the line card boot up time. MP will attempt to recover TM XPP link errors by executing resets and then keeping reset cards down that fail to recover after 3 resets.

Thus TM-XPP link is monitored at boot-up, and recovery action is performed. This check will be placed in periodic TM XPP link monitoring to catch link issues at run time and perform appropriate recovery.

This feature is supported for the following line cards:

- 8x10GbE
- 20x10-GbE/1GBE (M) / FRU# 53-1003238-xx
- 20x10-GbE/1GbE (X2) / FRU# 53-1003275-xx

- 24x10GbE
- 4x40GbE
- 2x100GbE

Enabling TM-XPP link monitoring

To enable TM XPP link monitoring, enter the **sysmon tm nif-check** command as shown in the following section.

sysmon tm nif-check

Syntax

sysmon tm nif-check threshold *count polling period*

[no] sysmon tm nif-check threshold *count polling period*

Two recovery actions are possible which are listed below:
sysmon tmnif-check action disable-ports

NOTE
disable-ports is default action.

[no] sysmon tmnif-check actionreset-linecard

Parameters

count
Number of link error events occurred within this polling period.

polling period
Period for polling.

Examples

For the Syslog default action:

```
Mar 4 20:33:57:A:System: LP15/TM0: All ports down due to TM XPP  link down
Mar 4 20:33:57:I:System: Interface ethernet 15/4, state down - TM XPP  link down
Mar 4 20:33:57:I:System: Interface ethernet 15/3, state down - TM XPP  link down
Mar 4 20:33:57:I:System: Interface ethernet 15/2, state down - TM XPP  link down
Mar 4 20:33:57:I:System: Interface ethernet 15/1, state down - TM XPP  link down
```

For the SNMP trap default action:

```
Health Monitoring: LP15: all ports down due to TM- XPP NIF link down
```

For the Syslog line card reset action:

```
Mar 4 20:33:57: D:System: Module reset in slot 1, triggered by TM Health Monitoring
Mar 4 20:33:57: D:System: TM Health Monitoring detects an issue in slot 1 ppcr 1 TM XPP  link down
```

For the SNMP trap line card action:

```
Type- debugging
System: Module reset in slot 1, triggered by TM Health Monitoring
```

History

Release version	Command history
R05.7.00b	This command was introduced.

Using alarms to collect and monitor device status

Beginning in the Extreme NetIron software R05.3.00, the software keeps two logs; one of hardware status currently available to the system, and another of hardware status history. The current alarm log keeps only entries for current information; when a hardware status is no longer valid, the entry is cleared. The alarm history log keeps a record of hardware statuses even after the status has changed. The alarm history log enables you to quickly determine trouble areas in a system. For example, by accessing the history, you can quickly determine if a problem is occurring too frequently and might require action.

Each hardware status entry is called an alarm and is classified by severity assigned by the software. The software categorizes alarms in the following levels:

- Critical - A condition that will cause damage to the system. A condition that causes a traffic outage on multiple ports.
- Major - A condition that causes traffic outage on single ports or might cause damage to the system.
- Minor - A condition that should be investigated but will not damage the system.

By default, all hardware status alarm levels of major severity and higher are logged, though you can configure the status alarm levels sent to both alarm logs (current and history). You can use the **show alarm** command to view the current status on a device, or a logged history of hardware alarms. To change the levels of alarms sent to the alarm logs, refer to Configuring Alarm History Buffer Size on page 228.

The alarms are specific to hardware status, whereas the syslog records information for software events. Alarms can also be configured on very specific terms such as a failed temperature sensor on a single interface module.

To take advantage of this feature, you should first set the alarm history buffer size. This is optional, but you have the option to limit how many entries are stored in the alarm history so you can free up space for other resources. Refer to Configuring Alarm History Buffer Size on page 228 for more information.

Next, you should configure the severity of alarms for each device you want logged. For detailed information, refer to Configuring alarm logging on page 229. Once you have configured your alarm logging, you can display alarms in the current alarm log and alarm history log using the show alarm command, as described in Displaying alarms on page 229.

Configuring Alarm History Buffer Size

The history buffer size is configurable. The default buffer size is 400 entries, but it can be configured to list between 100 and 3000 entries using the **alarm history** command.

For example, to configure the alarm history log size to 100 entries, enter the following command:

```
device# alarm history 100
```

Syntax: [no] alarm history *n*

where *n* is the number of log entries you want to store in the alarm history log, between 100 and 3000.

To reset the alarm history back to the default buffer size, use the **alarm history** command with the **no** operand. For example, to set the buffer size back to the default entry size from 100, enter the following command:

```
device# no alarm history 100
```

Configuring alarm logging

You can configure the system to log only specific level alarms for specific devices using the **alarm** command. The configuration setting applies to both logs, the current and history alarm logs. The level you set is the minimum level of alarms that will be logged. For example, if you set the configuration to log a minimum of minor level events, all minor, major and critical events will be logged. If you set the configuration to log a minimum of major level events, all major and critical events will be logged. If you set the configuration to log a minimum of critical level events, only critical level events will be logged.

For example, to configure the system to log a minimum of major level alarms on an interface module in slot 1, optic in slot 9, enter the following command:

```
device# alarm lp 1 optic 9 major
```

Alarms of major and critical severity will be logged for the optic in slot 9 on interface module in slot 1.

To reset the alarm history severity logging back to the default severity level, use the **alarm** command with the **no** operand. For example, to reset the alarms for the example above back to default, enter the following command:

```
device# no alarm lp 1 optic 9 major
```

NOTE
You cannot configure alarm severity on a system wide basis; you must specify a specific device, such as a fan, power supply or optic device. Once an alarm is set to log a minimum alarm level, the show commands cannot display alarm levels of lower severity levels as the information is not logged.

Displaying alarms

This section describes how to display alarms. You can display alarms at a very basic or specific level. The alarm logs display alarms they have been configured to log. The alarm history log is displayed in chronological order starting with the most recent entry.

NOTE
By default, all hardware status alarm levels of major severity and higher are logged. If you have configured different levels to be logged, only those levels of alarms can be displayed using the **show alarm** command.

For example, to display all alarms on the system of major alarm level only, enter the following command:

```
device# show alarm severity major
Jan  3 15:01:44 | Major    | Chassis | Power-Supply 2  - Not Present
Jan  3 15:01:44 | Major    | Chassis | Power-Supply 3  - Not Present
Jan  3 15:03:54 | Major    | LP   1  | Optic 1  - Alarm
Jan  3 15:02:21 | Major    | LP   1  | Optic 2  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 5  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 7  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 8  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 10 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 11 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 12 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 13 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 14 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 16 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 17 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 18 - Not Present
```

To display all alarms on the system of all alarm levels (as per your configured alarm severity logging), enter the following command:

```
device# show alarm all
Jan  3 15:01:44 | Major    | Chassis | Power-Supply 2  - Not Present
Jan  3 15:01:44 | Major    | Chassis | Power-Supply 3  - Not Present
Jan  3 15:03:54 | Major    | LP   1  | Optic 1  - Alarm
Jan  3 15:02:21 | Major    | LP   1  | Optic 2  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 5  - Not Present
```

```
Jan  3 15:02:21 | Major    | LP   1  | Optic 7  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 8  - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 10 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 11 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 12 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 13 - Not Present
Jan  3 15:02:21 | Major    | LP   1  | Optic 14 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 16 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 17 - Not Present
Jan  3 15:02:22 | Major    | LP   1  | Optic 18 - Not Present
```

The following table describes how to use the **show alarm** command to display alarm information.

TABLE 47 Displaying alarm log information

Description	Syntax
To display the default alarm levels.	**show alarm** `default`
To display all current alarms of a specific severity:critical, major, or minor. Alarms displayed depend on what you have configured the alarm logs to record.	**show alarm** `severity [ critical | major | minor ]`
Use to display all alarms in the alarm logs. Use the history operand to display the alarm history log.	**show alarm** `[history] all`
To display all alarms in the alarm log for all devices in the chassis. Alarms displayed depend on what you have configured the alarm logs to record.	**show alarm** `[history] chassis all`
To display all alarms in the alarm log related to all subsystems within the chassis or events for a particular subsystem(where subsystem is power supply or fan)(where x is the device number)	**show alarm** `[history] chassis subsystem all | x`
To display all alarms in the alarm log for all management modules and subsystems for the management modules.	**show alarm** `[history] mp all`
To display all alarms in the alarm log related to a specific management module (where *n*, module number is 1-3 for MLX/XMR and 1 for CER/CES) and all alarms for it's subsystems.	**show alarm** `[history] mp n all`
To display all alarms in the alarm log related to temperature information for a management module (where *n*, module number is 1-3 for MLX/XMR and 1 for CER/CES)and a specific fan (where x, is the temperature device number).	**show alarm** `[history] mp n temperature [all | x]`
To display all alarms in the alarm log for all interface modules and subsystems for the management module.	**show alarm** `[history] lp all`
To display all alarms in the alarm log related to a specific interface module(where *n*, module number is 1-3 for MLX/XMR and 1 for CER/CES) and all alarms for it's subsystems.	**show alarm** `[history] lp n all`
To display all alarms in the alarm log related to subsystem information for an interface module (where *n*, module number is 1-3 for MLX/XMR and 1 for CER/CES) and either all events on a specific subsystem, or events for a particular subsystem(where subsystem is temperature or optic)(where *x*, is a the device number).	**show alarm** `[history] lp n subsystem [all | x]`
To display all alarms in the alarm log for all SFM and subsystems for the SFM.	**show alarm** `[history] sfm all`

TABLE 47 Displaying alarm log information (continued)

Description	Syntax
To display all alarms in the alarm log related to a specific SFM(where *n*, is SFM slot 1-8 for MLX/XMR) and all alarms for it's subsystems.	**show alarm** `[history] sfm n all`
To display all alarms in the alarm log related to SFM information for a specific SFM(where *n*, is SFM slot 1-8 for MLX/XMR) and either all events on a specific subsystem, or events for a particular subsystem(where subsystem is temperature or fabric-element)(where *x* is 1-4 for a fabric element device number).	**show alarm** `[history] sfm n subsystem [all | x]`

Management and interface modules

When a management module or interface module is removed from the chassis, a major level alarm is generated in the alarm history log. If the management module, interface module, or SFM is powered off, a critical level alarm is generated in the alarm history log.

When a module is removed or powered off, alarms for all subsystems of the module are cleared from the current alarm log. If a module is removed from the chassis, all alarms are cleared from the current alarm log, and memory associated to its subsystems is freed. When a module is added to the configuration, memory is reallocated.

Temperature

If temperature on the management module or interface module increases to the highest threshold, a major alarm is set. If temperature decreases below the highest threshold, the alarm is cleared from the current alarm log, and an additional alarm is sent to the alarm history log stating that the condition has been removed. If the temperature increases into shutdown range, a critical level alarm is reported and logged in the alarm logs.

Optics

Alarms and warnings are monitored only for optic devices that support optical monitoring. If optical monitoring is disabled, then no alarms are generated.

If an optic is removed or not present, a major alarm is reported and logged and any existing alarms are cleared from the current alarm log.

> NOTE
> Alarms are not generated for optic device insertion.

Switch fabric element

If a switch fabric element cannot be accessed, a major alarm is reported and logged.

Chassis fans, power supplies, and optics

If there is an indication that a single fan has failed, a major alarm is reported and logged on the tray. If an incompatible fan tray is detected, a major alarm is reported and logged on the tray. When a fan tray is removed, any existing alarms are cleared and a major alarm is reported and logged on the tray.

If a power supply is installed but powered down, a minor alarm is reported and logged. If a power supply is installed incorrectly, a major alarm is reported and logged. If a power supply is not present, a major alarm is reported and logged.

Clearing the alarm history log

Use the **clear alarm** command to remove some or all of the current alarms. Once the alarm is cleared, it is removed from the current alarm database and is no longer available even though the condition might still exist. The alarm is kept in the history log.

If you clear all alarms, a single entry is added to the history that indicates all alarms have been cleared.

To clear all alarms from the alarm logs, enter the following command:

```
device# clear alarm all
```

For example, if you want to clear all alarms from the alarm logs on a specific optic in slot 9 of the interface module in slot 1, enter the following command:

```
device# clear alarm lp 1 optic 9
```

Disabling SNMP trap generation and logging

With the introduction of the alarm feature, you may want to disable some SNMP trap generation and logging to save space.

To disable SNMP fan change-trap generation, enter the following command:

```
device(config)# no snmp-server enable traps fan-speed-change
```

To disable Syslog fan-speed-change logging, enter the following command:

```
device(config)# no logging enable fan-speed-change
```

For additional information on SNMP traps and logging, refer to the *Extreme NetIron MIB Reference* .

Displaying MR2 management module memory usage

In Extreme NetIron software R05.3.00 and later, you can use all 4G of physical memory on the MR2 management module. To display MR2 memory usage, enter the following command:

```
device# show mem
ID   Memory Used   Available     Success    Hold     Fail    Error
   0 21401600      14397440      1508      633       0        0         OS
   1 51474432      216961024     22        22        0        0         Shared
   2 107184128    2747834368     25969     10813     0        0         Global
   3  0            267386880     0         0         0        0         User Private
   4  0            267386880     0         0         0        0         Priv4
   5  0            267386880     0         0         0        0         Priv5
   6  0            267386880     0         0         0        0         Priv6
   7  0            267386880     0         0         0        0         Priv7
   8  0            267386880     0         0         0        0         Priv8
   9  0            267386880     0         0         0        0         Priv9
  10  0            267386880     0         0         0        0         Priv10
  11  0            267386880     0         0         0        0         Priv11
  12  0            267386880     0         0         0        0         Priv12
   - 19722240      47386624      10        10        0        0         DMA
  Total Installed: 4294967295, Total Free: 3988713472
```

Syntax: show memory

Enabling and disabling management module CPU usage calculations

You can enable the router to perform usage averaging calculations on tasks handled by CPU on the management module. You can then display usage averages for all tasks performed by the CPU on the management module for an interval of up to one hour. You can display these statistics using the **show cpu** command.

> NOTE
> Typically, these statistics are used for debugging purposes.

By default, the performance of the calculations is disabled. When disabled, you can use the **show cpu** command without optional parameters to display usage averages for all tasks performed by CPU on the management module.

> NOTE
> The **cpu-usage** command must be configured in order to poll the MP CPU utilization.

To enable the usage averaging calculations, enter the following command at the global CONFIG level of the CLI.

```
device(config)# cpu-usage on
```

Syntax: cpu-usage on

To disable the usage averaging calculations, enter the following command at the global CONFIG level of the CLI.

```
device(config)# cpu-usage off
```

Syntax: cpu-usage off

Displaying CPU usage

Use the **show cpu** command to display usage averages for all tasks performed by the management module as shown in this example.

```
device# show cpu
... Usage average for all tasks in the last 1 seconds ...
==========================================================
Name                     us/sec           %
idle                     755423          100
monitor                  13              0
wd                       46              0
flash                    0               0
dbg                      6               0
boot                     92              0
main                     0               0
itc                      0               0
tmr                      588             0
ip_rx                    211             0
scp                      36              0
console                  54              0
vlan                     0               0
mac_mgr                  38              0
mrp                      0               0
vsrp                     0               0
snms                     71              0
rtm                      640             0
rtm6                     40              0
ip_tx                    2478            0
rip                      0               0
mpls                     119             0
nht                      0               0
mpls_glue                13              0
```

```
bgp                     0               0
bgp_io                  0               0
ospf                    737             0
ospf_r_calc             0               0
isis                    38              0
isis_spf                0               0
mcast                   18              0
msdp                    134             0
vrrp                    0               0
ripng                   0               0
ospf6                   66              0
ospf6_rt                0               0
mcast6                  7               0
bfd                     0               0
l4                      98              0
stp                     0               0
gvrp_mgr                0               0
snmp                    0               0
rmon                    13              0
web                     86              0
lacp                    0               0
dot1x                   0               0
dot1ag                  7               0
hw_access               1049            0
ospf_msg_task           0               0
telnet_0                0               0
telnet_1                44              0
```

Syntax: show cpu

Displaying management module CPU usage

You can display the tasks handled by the management module and the amount of the management module CPU used by each task by entering the **show tasks** command at any level of the CLI.

```
device# show tasks
Task Name   Pri   State     PC      Stack     Size  CPU Usage(%) task id  task vid
----------  ---  -----  ---------  --------  -----  ---------   ------   -------
       idle 0      run  00001904  040560a0  256     66          0        0
    monitor 20    susp  0000c658  0404bd80  8192    0           0        0
        int 16    susp  0000c658  04051f90  16384   0           0        0
      timer 15    susp  0000c658  04055f90  16384   0           0        0
        dbg 30    susp  0000c658  0404df10  8192    0           0        0
      flash 17    susp  0000c658  0409cf98  8192    0           0        0
         wd 31    susp  0000c658  0409af80  8192    0           0        0
       boot 17    susp  0000c658  041dbe30  65536   0           0        0
       main 3     susp  0000c658  2060cf38  65536   0           0        1
        itc 6     susp  0000c658  20610af0  16384   0           0        1
        tmr 5     susp  0000c658  206a7638  16384   0           0        1
      ip_rx 5     susp  0000c658  206aef48  16384   0           0        1
        scp 5     susp  0000c658  206b3638  16384   0           0        1
    console 5     susp  0000c658  206bf628  32768   0           0        1
       vlan 5     susp  0000c658  206c6628  16384   0           0        1
    mac_mgr 5     susp  0000c658  206d5638  16384   0           0        1
    mrp_mgr 5     susp  0000c658  206db638  16384   0           0        1
       vsrp 5     susp  0000c658  206e1630  16384   0           0        1
       snms 5     susp  0000c658  206e5638  16384   0           0        1
        rtm 5     susp  0000c658  20756638  16384   0           0        1
      ip_tx 5      run  0000c658  20763638  16384   0           0        1
      mcast 5     susp  0000c658  20767638  16384   0           0        1
         l4 5     susp  0000c658  2076b630  16384   0           0        1
        stp 5     susp  0000c658  20970628  16384   0           0        1
   gvrp_mgr 5     susp  0000c658  20979638  16384   0           0        1
       snmp 5     susp  0000c658  20982638  32768   0           0        1
        web 5     susp  0000c658  2098d638  32768   0           0        1
       lacp 5     susp  0000c658  20991638  16384   0           0        1
```

```
hw_access 5     susp  0000c658  20996638  16384   0           0        1
 telnet_0 5      run  0000c658  209db638  32768   0           0        1
```

Syntax: show tasks

Examine the CPU Usage (%) field to determine the percentage of management module CPU used by each task.

> NOTE
> The total CPU usage may not add up to 100 percent. The total may not include resources used by the management processes.

A problem could exist If the CPU usage is distributed unevenly to one task, other than the idle task, for a prolonged period. If this situation occurs, contact Extreme Networks Technical Support for assistance.

Removing MAC address entries

You can remove the following learned MAC address entries from the system MAC address table:

- All MAC address entries
- All MAC address entries for a specified interface module
- All MAC address entries for a specified Ethernet port
- All MAC address entries for a specified VLAN
- A specified MAC address entry in all VLANs

For example, to remove entries for the MAC address 000d.cb80.00d in all VLANs, enter the following command at the Privileged EXEC level of the CLI.

```
device# clear mac-address 000d.cb80.00d0
```

Syntax: clear mac-address *mac-address* [**ethernet** *slot-num/port-num*] | [**module** *slot-num*] | **vlan** *number*

- If you enter the **clear mac-address** command without any parameters, the software removes all MAC entries.
- Use the **mac-address** parameter to remove a specified MAC address from all VLANs. Specify the MAC address in the following format: HHHH.HHHH.HHHH.
- Use the **ethernet***slot-num* or *port-num* parameter to remove all MAC addresses for a specified Ethernet port. For the *slot* parameter, enter the number of the device slot in which the Ethernet interface module is installed. For the *port* parameter, enter the Ethernet port for which to remove all MAC addresses.
- Use the **module***slot-num* parameter to remove all MAC addresses for an interface module in a specified device slot.
- Use the **vlan***number* parameter to remove all MAC addresses for a specified VLAN.
- If you enter the **clear mac-address** command without any parameters, the software removes all MAC entries.
- Use the **mac-address** parameter to remove a specified MAC address from all VLANs. Specify the MAC address in the following format: HHHH.HHHH.HHHH.
- Use the **ethernet***slot-num* or *port-num* parameter to remove all MAC addresses for a specified Ethernet port. For the *slot* parameter, enter the number of the device slot in which the Ethernet interface module is installed. For the *port* parameter, enter the Ethernet port for which to remove all MAC addresses.
- Use the **module***slot-num* parameter to remove all MAC addresses for an interface module in a specified device slot.
- Use the **vlan***number* parameter to remove all MAC addresses for a specified VLAN.

IPv6 ND Proxy

Enabling the ND proxy feature causes the router to reply on behalf of the target host (if the target host exists).

For nodes on different segments, the NS request for resolving the neighbor may not reach another host. The reply will contain the link-local address of the router interface which is sending the reply, instead of the link-local address of the target host.

When any IPv6 packet is received on a proxy interface, it must be parsed to see whether it is known to be one of the following types:

- ICMPv6 Neighbor Solicitation (NS)

  If the received packet is an ICMPv6 Neighbor Solicitation (NS), the NS is processed locally but no NA is generated immediately. Instead the NS is proxied, and the NA will be proxied when it is received. This ensures that the proxy does not interfere with hosts moving from one segment to another, since it never responds to an NS based on its own cache.
- ICMPv6 Neighbor Advertisement (NA)

  If the received packet is an ICMPv6 Neighbor Advertisement (NA), the neighbor cache on the receiving interface is first updated as if the NA were locally destined, and then the NA is proxied.

ND Proxy Example

In the following topology, A and B are nodes on separate segments which are connected by proxy P.

- A and B have link-layer addresses a and b, respectively.
- P has link-layer addresses p1 and p2 on the two segments.

```
A---|---P---|---B
 a    p1 p2    b
```

When A attempts to send an initial IPv6 packet to B, the following actions occur:

- Route look up for destination address **B** is executed on **A**. Before the packet can be sent, **A** needs to resolve **B**'s link-layer address and sends a Neighbor Solicitation (NS) to the solicited-node multicast address for **B**. The Source Link-Layer Address (SLLA) option in the solicitation contains **A**'s link-layer address.
- **P** receives the solicitation (since it is receiving all link-layer multicast packets) and processes it. Since it is an NS, it creates a neighbor entry for **A** on interface 1, and records its link-layer address. It also creates a neighbor entry for **B** (on an arbitrary proxy interface) in the *INCOMPLETE* state. Since the packet is multicast, **P** then needs to proxy the NS out on all other proxy interfaces on the subnet. Before sending the packet out on interface 2, it replaces the link-layer address in the SLLA option with its own link-layer address of **p2**.
- **B** receives this NS, processing it as usual. A neighbor entry for **A** is created and mapped to the link-layer address **p2**. In response, a Neighbor Advertisement (NA) is sent to **A** containing **B**'s link-layer address **b**. The NA is sent using **A**'s neighbor entry, i.e. to the link-layer address **p2**.
- The NA is received by **P**, which is processed as would occur with any unicast packet; i.e. the NA is forwarded out of interface 1, based on the neighbor cache. However, before actually sending the packet out, it is inspected to determine if the packet about to be sent is one that requires proxying. Since it is an NA, it updates its neighbor entry for **B** to be *REACHABLE* and records the link-layer address **b**. **P** then replaces the link-layer address in the LLA option with its own link-layer address on the outgoing interface, **p1**. The packet is then sent out on interface 1.
- When **A** receives this NA, it is processed as usual. Hence a neighbor entry is created for **B** on interface 1 in the *REACHABLE* state, and the link-layer address **p1** is recorded.

IPv6 ND Proxy Configuration Tasks

The IPv6 ND Proxy is configured through the tasks of turning on the proxy capability for the node (**ipv6 nd proxy**), and defining the IPv6 destination network (**ipv6 route**). This configuration requires defining the outgoing interface as **ethernet** (with the *slot* or *port*), or **ve** (with the *ve-id*).

The commands for this configuration task are introduced at the configuration command level, and used to configure ipv6 static route by specifying the destination prefix and outgoing interface. As per the topology mentioned in the packet flow if the proxy is configured on R2, this static route can be configured on R1 with a destination prefix of 2002::/64. The static route can also be configured **ve** as an outgoing interface.

NOTE
Support for the **ipv6 nd proxy** command is as follows:

- Not supported over an v6 tunnel interface.
- Currently supported for NS and NA messages.
- Not supported for ND messages such as RS, RA, and redirect messages.

1. ipv6 nd proxy

   The following step example shows a typical **ipv6 nd proxy** configuration command sequence executed from the configuration command level.

   Example:

```
R2>
R2>en
No password has been assigned yet...
R2#conf t
R2(config)# ipv6 nd proxy
R2(config)#
```

2. **ipv6 route** *<X:X::X:X/M>* [**ethernet**| **ve**] [*slot/port* | *ve_id*]

   The following step examples show typical **ipv6 route** configuration command sequences executed from the configuration command level.

   Example 1:

```
R1(config)#
R1(config)#ipv6 route 2002::/64 ethernet 1/1

R1(config)#
R1(config)#ipv6 route 2003::/64 ve 10

R1(config)#vrf green
R1(config-vrf-green)#address-family ipv6
R1(config-vrf-green-ipv6)#ipv6 route 2002::/64 eth 1/1

R1(config)#vrf green
R1(config-vrf-green)#address-family ipv6
R1(config-vrf-green-ipv6)#ipv6 route 2003::/64 ve 10
```

   Example 2:

```
R1#show running-config    ( Truncated output showing only static route)

ipv6 route 2002::/64 ethernet 1/1
ipv6 route 2003::/64 ve 10

vrf green
 rd 66:66
 address-family ipv6
 ipv6 route 2002::/64 ethernet 1/1
 ipv6 route 2003::/64 ve 10
exit-vrf
```

ipv6 nd proxy

Configures a single IPv6 subnet prefix to support multiple physical links in IPv6 Neighbor Discovery.

Syntax

ipv6 nd proxy

no ipv6 nd proxy

Command Default

This feature is disabled.

Modes

The `ipv6 nd proxy` is configurable under the global configuration mode.

Usage Guidelines

The IPv6 ND proxy command turns on the IPv6 ND proxy capability for the node, and is run at the configuration level.

Use the **no** form of this command to remove the ND proxy configuration.

Per RFC 4389, ND proxy can be used to bridge multiple links into a single entity to simplify management, as there is no need to allocate subnet numbers to the different networks. This can help alleviate the need to configure NAT in IPv6 networks.

> NOTE
> This is an IETF Experimental Protocol. It is the responsibility of the user to ensure that appropriate network-layer support is provided.

The following limitations apply:

- The `ipv6 nd proxy` is not supported over v6 tunnel interface.
- The `IPv6 nd proxy` programs the RACL to force the Unicast NS, sent during neighbor refresh, to the CPU for processing as proxy NS.
- The `ipv6 nd proxy` is currently supported for NS and NA messages and are not supported for other ND messages like RS, RA and redirect message.
- The `IPv6 nd proxy` is not supported for the IPsec tunnels and on MCT.

Examples

To enable the `IPv6 ND proxy` feature for the node:

```
R2>#en
No password has been assigned yet...
R2#conf t
R2(config)# ipv6 nd proxy
R2(config)#
```

ipv6 nd local-proxy

Configures an IPv6 interface to support IPv6 ND local proxy.

ipv6 nd local-proxy

no ipv6 nd local-proxy

This feature is disabled.

The `ipv6 nd proxy` is configurable under the global configuration mode.

The `IPv6 ND local-proxy` command is supported over the VE interface. It is not supported for the VEoVPLS interface.

Use the **no** form of this command to remove the `IPv6 ND local-proxy` configuration.

Limitations and pre-requisites

The `ipv6 nd local-proxy` command is supported for the VE interface, but not for the VE over VPLS interface.

To enable the `IPv6 ND local-proxy` feature for the node:

```
R2>#en
No password has been assigned yet...
R2#conf t
R2(config)#int eth3/1
R2(config-if-e10000-3/1)#ipv6 nd local-proxy
R2(config-if-e10000-3/1)#
```

ipv6 route

Configures a static IPv6 route for an interface.

Syntax

ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*link-local-next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*link-local-next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 route *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*link-local-next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*link-local-next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

Command Default

An IPv6 static route is not configured.

Parameters

dest-ipv6-prefix
: Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length
: A decimal value specifying the length of the IPv6 prefix.

next-hop-ipv6-address
: IPv6 address of the next-hop gateway.

link-local-next-hop-ipv6-address
: IPv6 address of the link-local next-hop gateway.

next-hop-vrf *vrf_name next-hop-ipv6-address*
: Specifies a VRF instance and a next-hop IPv6 address.

null0
: Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

ethernet *slot/port*
: Specifies the Ethernet slot or port.

ve *ve-id*
: Specifies the virtual Ethernet (VE) interface VE ID.

6to4_tnl *tunnel-id*
Specifies IPv6 to IPv4 tunnel number to be used as next hop.

ipv6_tnl *tunnel-id*
Specifies IPv6 tunnel to be used as next hop.

name *string*
Optional name (ASCII string) assigned to the route

metric
Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*
Specifies an administrative distance. The range is from 1 through 255. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route.

tag
Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number
A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command removes the IPv6 static route. If the route is named, the **no** command must be used twice, the first time to remove the name and the second time to remove the route.

Examples

To configure the IPv6 ND proxy static route by specifying the destination prefix and the outgoing interface:

> **NOTE**
> As per the topology mentioned in the packet flow, if the IPv6 ND proxy is configured on R2, then this static route can be configured on R1 with the destination prefix being 2002::/64. The static route can also be configured with outgoing interface as **ve**, such as **ve 10**.

```
R1(config)#
R1(config)# ipv6 route 2002::/64 ethernet 1/1

R1(config)#
R1(config)# ipv6 route 2003::/64 ve 10

R1(config)# vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2002::/64 eth 1/1

R1(config)#vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2003::/64 ve 10
```

To **show** the **running-config** (with truncated output showing only the static route):

```
R1(config)# ipv6 route 2002::/64 ethernet 1/1
R1(config)# ipv6 route 2003::/64 ve 10

vrf green
 rd 66:66
 address-family ipv6
 ipv6 route 2002::/64 ethernet 1/1
 ipv6 route 2003::/64 ve 10
R1(config)#exit-vrf
```

DRBG Health Test on IPsec LP

Deterministic Random Bit Generator (DRBG) health and error checks are performed on the IPsec line card used in the MLX Series devices.

The FIPS self-test is executed at system startup, which includes DRBG health and error checks. This startup test executes a known answer test, which includes DRBG health and error checks.

The DRBG Known Answer Test (KAT) and health test are performed during:

- System boot-up and at regular intervals.
- Periodic testing after 2^24 uses, during instantiate and reseed.
- DRBG check immediately after powering on the system.

The type of DRBG mechanism and the cryptographic primitives used (e.g., AES-128 or SHA-256), are as follows:

- Type of DRBG mechanism: Hash Based
- Cryptographic primitives used: SHA-256

Security strengths of the cryptographic algorithms supported by the implementation: 256

The implementation of this feature (e.g., prediction resistance, personalization string, additional input) are as follows:

- Prediction Resistance is not TRUE.
- Personalization String Length = 0
- Additional Input Length = 0

NOTE

The DRBG mechanism functions are not distributed. `CTR_DRBG` is not used on IPsec LP.

Maintenance and Field Replacement

- Maintenance and field replacement overview....245
- Hardware maintenance schedule....245
- Replacing a management module....246
- Replacing an interface module....247
- Replacing a switch fabric module....248
- Replacing a fiber-optic transceiver....248
- Replacing a power supply....249
- Replacing fan assemblies....255

Maintenance and field replacement overview

This chapter describes how to perform any required maintenance on your device. It also describes how to install the following field-replaceable hardware:

- Management modules
- Compact flash cards in management modules
- Interface modules
- Switch fabric modules
- Fiber optic transceivers
- Fans
- Power supplies
- Fan deflectors
- Air filters

Hardware maintenance schedule

DANGER
The procedures in this manual are for qualified service personnel.

Extreme routers require minimal maintenance for hardware components. It is recommended that you perform the following regular maintenance tasks:

- Clean the fiber-optic connectors on a fiber-optic transceiver port and the connected fiber cable each time you disconnect the cable.
- Replace the air filters quarterly.

You can also replace the following hardware components, as needed:

- All modules (management, interface, and switch fabric).
- Fiber-optic transceivers.
- AC or DC power supplies.
- Fan assemblies.

NOTE
The management, interface, and switch fabric modules are dedicated, which means that you must install them in Extreme routers only. If you install these modules in another Extreme device or you install a module intended for another Extreme device in a Extreme router, the device and modules will not function properly.

Replacing a management module

For instructions on how to install or replace modules, refer to the module installation section in the installation chapter for your router model.

Installing the Compact Flash Card in an MR2 management module

MR2 management modules allow users to insert an additional 2 Gbps compact flash card. To install the card, you need a flat head or Philips screw driver. Refer to the following figure to see where the slot card should be placed.

NOTE
MR and MR2 management modules should not be used together in the same chassis. Please read the Hardware Installation Notes that came with your hardware before installing the MR2 management module. The internal compact flash card cannot be accessed for removal or replacement. To obtain a replacement or a new compact flash card, contact Extreme technical support.

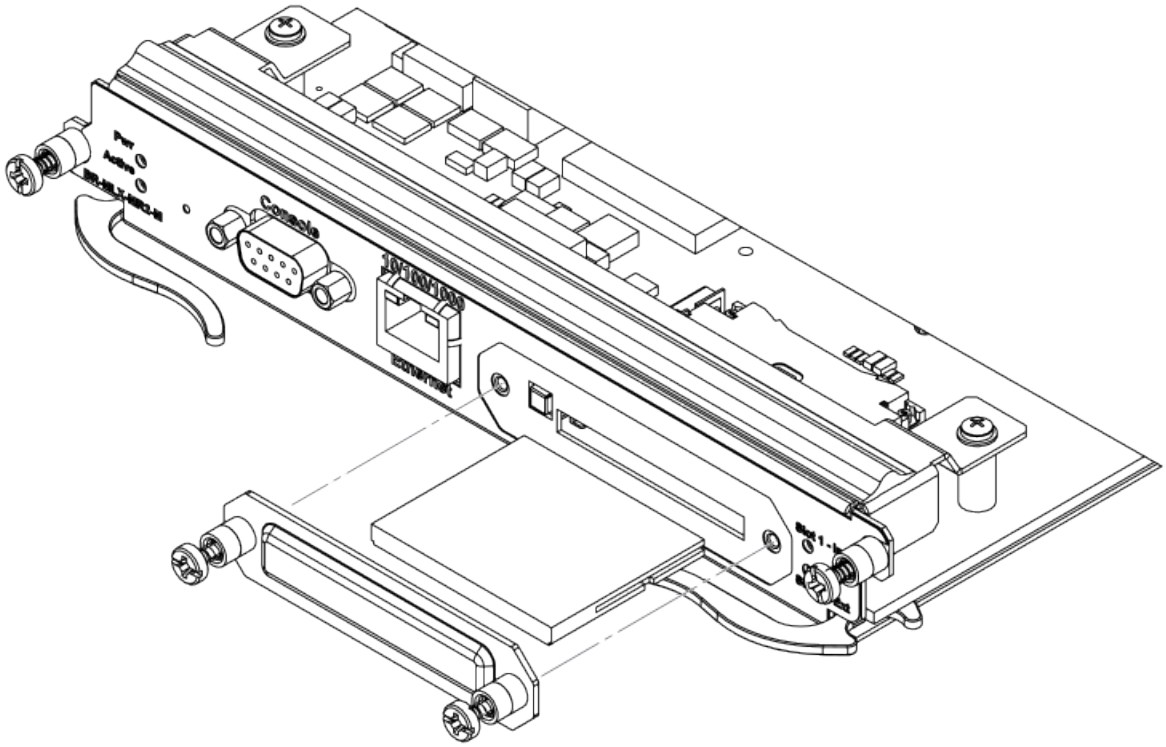
To install a compact flash card in an MR2 management module:

1. Remove the two screws holding the compact flash card cover in place using a flat head or Phillips screw driver.

   Put the screws and cover plate aside; you will need to reattach the cover using the screws after installing the card.
2. Slide the compact flash card into the slot.

3. Reattach the cover plate using the two screws and screwdriver.

FIGURE 108 Inserting a compact flash card in the MR2 management module



Replacing an interface module

You can remove or replace interface modules while the router is powered on and running. For more information on module slot locations, refer to Product Overview on page 21.

> NOTE
> It is not recommended that you hot-swap an interface module that is running a software image older or newer than the image on the management module. Although the management module will attempt to sync the application image on the interface module, it may not be able to sync older FPGA images. In this case the interface module may attempt to continuously reload. Always upgrade or downgrade the FPGA images on replacement interface modules to match the software version on the management module before you install the interface modules in your device.

For information about how to install a new or replacement module, refer to the installation chapter for your router model.

> NOTE
> If you are hot-swapping a component, allow a minimum of two seconds after a component has been removed before inserting a replacement component in the same slot.

Removing and replacing an interface module

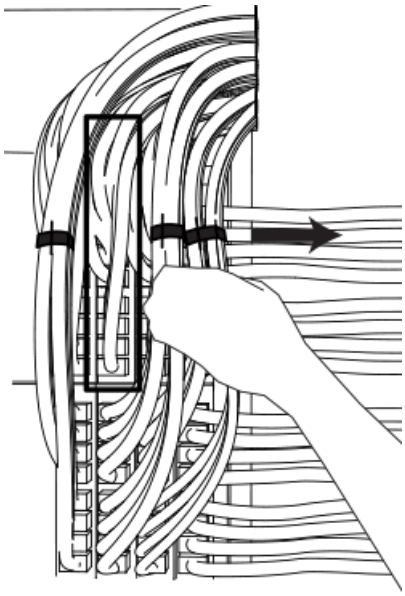
To remove or replace an interface module, see the module instructions in the installation chapter that is appropriate for your router model.

For 16-slot routers, if you insert a module into a slot where the fan speed for a previous module was manually configured, you will need to change the fan speed back to auto. For example, if the fan speed was manually configured to "slow", and you are installing a module that requires more cooling power, the "slow" setting will cause the module to overheat. To configure the fan speed to auto, enter the **set fan speed auto** command.

```
device# set-fan-speed auto
```

Due to the high cable capacity of 32-slot routers, cable bundles can be very dense. The design of the cable management system allows you to access interface modules in the top row of the upper card cage without having to disconnect cables from the bottom row of the same card cage. Simply move the cable bundles from the lower card cage to the side, as shown in the following figure.

FIGURE 109 Accessing the interface modules on a fully-loaded 32-slot chassis



Replacing a switch fabric module

You can replace a switch fabric module while the router is powered on and running. For more information on switch fabric slot locations, refer to Switch fabric modules on page 75. For installation instructions for switch fabric modules, see the installation chapter that is appropriate for your router model.

> NOTE
> If you are hot-swapping a component, please allow a minimum of two seconds after the old component has been removed before inserting a replacement component in the same slot.

For a graceful shutdown of the links, it is recommended that you disable the switch fabric module before removing it from the device. It is also recommended that you remove or replace switch fabric modules one at a time. If you need to remove all of the switch fabric modules at the same time, you must shut down the router and remove the power source.

Replacing a fiber-optic transceiver

You can replace a fiber-optic transceiver in a 10 Gigabit Ethernet port while the device is powered on and running.

DANGER
All fiber-optic interfaces use Class 1 lasers.

DANGER
Laser Radiation. Do Not View Directly with Optical Instruments. Class 1M Laser Products.

Before removing a fiber-optic transceiver, have the following items available:

- The protective covering that you removed from the fiber-optic transceiver port when you initially installed the module
- An ESD wrist strap with a plug for connection to the ESD connector on the router chassis.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

To replace a fiber-optic transceiver in a 10 Gbps Ethernet port, perform the following steps:

1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector located on the front of the router.
2. Disconnect the two fiber cable connectors from the port connectors.
3. Replace the protective cover on the port connectors.
4. Pull down the latch on the front of the transceiver.
5. Pull the transceiver out of the port and place it in an anti-static bag for storage.
6. Remove the new transceiver from the protective packaging.
7. Insert the fiber-optic transceiver into the port until it clicks into place. Fiber-optic transceivers are keyed to prevent incorrect insertion.

Cabling a fiber-optic transceiver

To cable a fiber-optic transceiver, perform the following steps:

1. Before cabling a fiber-optic transceiver, it is strongly recommended that you clean the cable connectors and the port connectors. For more information, refer to Cleaning fiber-optic ports and connectors on page 198.
2. Gently insert the two cable connectors (a tab on each connector should face upward) into the port connectors until the tabs lock into place.

Replacing a power supply

You can replace a power supply while the device is powered on and running. For the location of the power supplies (AC or DC) refer to Power supplies on page 79.

NOTE
If you are hot-swapping a module, power supply, or fan tray, allow a minimum of two seconds after a module (or power supply or fan tray) has been removed before inserting a module in the same slot.

Determining which power supply failed

To determine which power supply has failed, enter the **show chassis** command at any CLI command prompt.

```
device# show chassis
```

This command displays status information for the fans and power supplies, and temperature readings for various components in the device. The power supplies are numbered in the display. Refer to Displaying device status and temperature readings on page 204 for more information.

If a power supply has failed, the display indicates "Installed (Failed)" and identifies the slot in which the failed power supply is installed.

Setting the threshold for power supply monitoring

The **power-supply monitoring threshold** command monitors the power supply state, and indicates when a power supply will shut down due to failure.

To set a threshold value for power supply monitoring, enter the following command.

```
device(config)#power-supply monitoring threshold 3
A Power Supply will be Shutdown if it fails 3 times within an Hour
```

The power supply will flap three times within an hour, after which the power supply will automatically shut down.

Syntax: [no] power-supply monitoring [**threshold** *decimal*]

The *decimal* variable specifies the number of flaps within an hour after which a power supply will automatically shutdown. The threshold range is from 0 through 32. The default value is 5. A value of 0 disables the power supply auto-shutdown on flapping.

> NOTE
> A threshold value of 0 will not automatically shutdown a power supply due to failures.

For Syslog messages, please refer to Appendix A, Using Syslog in the *Extreme NetIron Management Configuration Guide*.

Clearing power supply failure timestamps

Use the **power-supply monitoring clear** command to clear all collected failure timestamps for a given power supply, or for all available power supplies.

To clear all collected failure timestamps for a power supply, enter the following command.

```
device(config)# power-supply monitoring clear 1
This will clear all collected failure timestamps for the Power Supply # 1
Are you sure? (enter 'y' or 'n'): y
```

To clear all collected failure timestamps for all available power supplies, enter the following command.

```
device(config)# power-supply monitoring clear all
This will clear all collected failure timestamps for all available Power Supplies
Are you sure? (enter 'y' or 'n'): y
```

You are asked to verify this command by entering "yes" or "no".

Syntax: power-supply monitoring clear *decimal* | **all**]

By default, no power-supply monitoring is configured.

The *decimal* variable specifies a power supply number, The **all** keyword clears all available power supplies.

Displaying power supply monitoring timestamps

To display timestamps for failures on any power supply, enter the following command.

```
device#show power-supply-monitoring
    PS-1     PS-2     PS-3     PS-4
```

```
1 ) 0         0         0         0
2 ) 0         0         0         0
3 ) 0         0         0         0
4 ) 0         0         0         0
5 ) 0         0         0         0
6 ) 0         0         0         0
7 ) 0         0         0         0
8 ) 0         0         0         0
9 ) 0         0         0         0
10) 0         0         0         0
11) 0         0         0         0
12) 0         0         0         0
13) 0         0         0         0
14) 0         0         0         0
15) 0         0         0         0
16) 0         0         0         0
17) 0         0         0         0
18) 0         0         0         0
19) 0         0         0         0
20) 0         0         0         0
21) 0         0         0         0
22) 0         0         0         0
23) 0         0         0         0
24) 0         0         0         0
25) 0         0         0         0
26) 0         0         0         0
27) 0         0         0         0
28) 0         0         0         0
29) 0         0         0         0
30) 0         0         0         0
31) 0         0         0         0
32) 0         0         0         0
Monitoring Threshold: 32 flaps/hour
```

In the example above, the configured power supply monitoring threshold is 32 cycles per hour.

You can also use the show running-config command to display the power supply monitoring threshold configuration, as displayed in the following example.

```
device#show running-config
Current configuration:
!
ver V5.4.0T163
module 1 br-mlx-2-port-100g-x
module 3 ni-mlx-48-port-1g-mrj21
!
!
!
no logging enable ntp
logging console
telnet login-retries 5
telnet server
power-supply monitoring threshold 32
username script password 8 $1$hR/..5B1$adiszoS76gLD9zIyFF1ER1
```

In the example above, the configured power supply monitoring threshold is 32 cycles per hour.

Use the following command to show the uptime of modules:

```
device#show version | include time
Active Management uptime is 9 minutes 30 seconds
Standby Management uptime is 8 minutes 45 seconds
LP Slot 3 uptime is 8 minutes 48 seconds
LP Slot 4 uptime is 8 minutes 48 seconds
LP Slot 5 uptime is 8 minutes 50 seconds
LP Slot 6 uptime is 8 minutes 50 seconds
LP Slot 8 uptime is 8 minutes 48 seconds
device#
device# show version | include xmr
Compiled on Jul  9 2012 at 09:52:52 labeled as xmr05400b396
```

```
Compiled on Jul  9 2012 at 09:52:52 labeled as xmr05400b396
device#
```

The **show power-supply-monitoring** command displays the last 32 recorded failure timestamps for a power supply. The displayed failure timestamp is the number of seconds since the last system reboot. The current configured power supply monitoring threshold value is also displayed at the end of the output.

Syntax: show power-supply-monitoring

Enabling a power supply shutdown

> NOTE
> The **power-on power supply** and **power-off power-supply** commands are not available on some power supplies. These commands can be useful for Extreme Technical Support when troubleshooting a router. It is recommended you use the commands only when troubleshooting a router with Extreme Technical Support.

The **power-off power-supply** command allows you to shut down a power supply manually.

To shut down a power supply, enter the following command.

```
device# power-off power-supply 3
This will Shutdown The Power Supply # 3
Are you sure? (enter 'y' or 'n'): y
ERROR: Power Supply # 3 is the Last Available in the system and will not be shutdown.
To force the shutdown, please use keyword "forced"
```

Syntax: power-off power-supply [**forced**] *decimal*

The **power-supply** keyword allows you to shut down a power supply.

The *decimal* variable specifies a power supply index number.

The forced option forces the last power supply available in the system to shut down. The CLI will not shut down the last power supply unless the **forced** option is used.

Powering on the power supply through the CLI

> NOTE
> The **power-on power supply** and **power-off power-supply** commands are not available on some power supplies. These commands can be useful for Extreme Technical Support when troubleshooting a router. It is recommended you use the commands only when troubleshooting a router with Extreme Technical Support.

Use the **power-on power-supply** command to turn on a power supply that has been shut down.

A power supply will shut down due to flapping, or if a shutdown is enabled manually using the **power-off power-supply** command. Refer to Enabling a power supply shutdown on page 252.

To turn on a power supply that has shut down, enter the following command.

```
device# power-on power-supply 1
AC Power Supply 1 is OK
```

The output example displays the status for power supply 1 as OK.

> NOTE
> If a power supply has shut down, power to the interface module may be lost, as there may not be enough power remaining in the system to keep the module powered.

Syntax: power-on [**power-supply** *decimal*]

The *decimal* variable specifies a power supply index number.

Replacing a power supply

To replace a power supply, have the following items available:

- A new power supply (AC or DC), which you can order from Extreme Networks.
- A small flat-blade or Phillips screwdriver (MLXe-4 and MLXe-32 modules)

CAUTION
Remove the power cord from a power supply before you install it in or remove it from the device. Otherwise, the power supply or the device could be damaged as a result. (The device can be running while a power supply is being installed or removed, but the power supply itself should not be connected to a power source.)

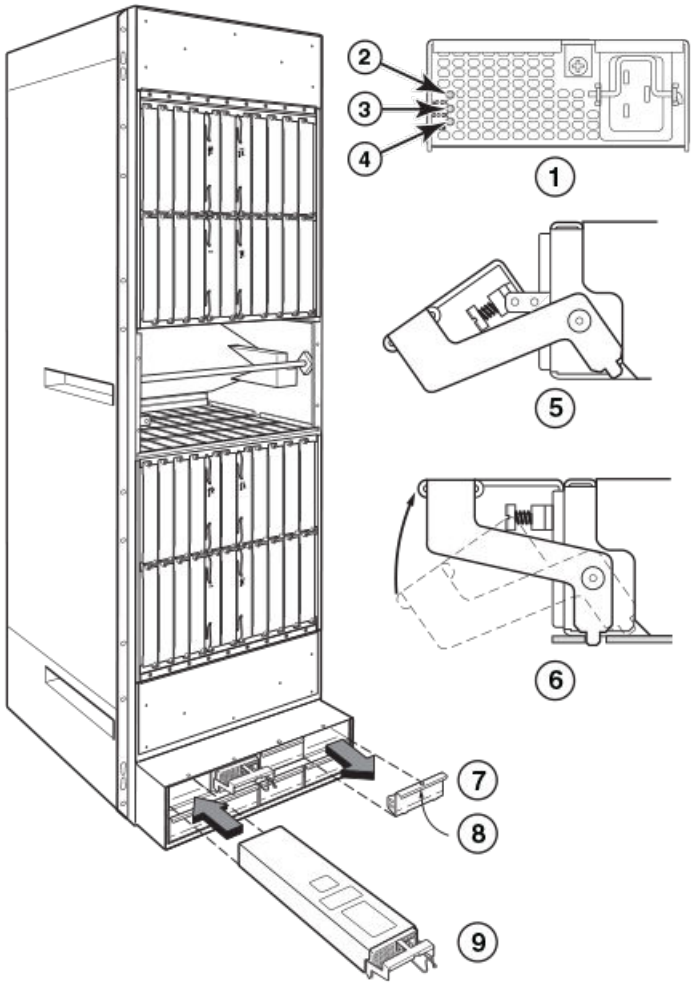
CAUTION
To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

1. Disconnect the power supply from the power source.
2. Disconnect the power cables from the power supply.

3. Remove the power supply from the device:
   - For a 4-slot device: Use the screwdriver to loosen the two screws on both sides of the power supply faceplate. Then pull the ejectors forward until the power supply disconnects from the backplane.
   - For an 8-slot or 16-slot device: Pull up on the plunger on the faceplate and pull the handle toward you until the power supply is released.
   - For a 32-slot device: Make sure the captured screw underneath the latch handle on the power supply faceplate is loose. Pull down on the latch handle and curl your fingers over the handle. Pull the handle straight out toward you to unlock the power supply (see the following figure).

   Pull the power supply out of the device.

FIGURE 110 Removing and replacing a power supply in an MLXe-32 device.



1	Power supply indicators	5	Latch handle open
2	AC power input LED (AC OK)	6	Lift up latch handle to lock
3	DC power output LED (DC OK)	7 & 8	Power supply blank cover
4	Alarm LED (ALM)	9	Power supply

4. Insert the new power supply into the empty power supply slot, using the guides provided on either side of the slot.

   CAUTION
   Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

5. After you insert the power supply, push gently on the power supply faceplate until the power supply is fully seated.
6. Pull up on the handle on the power supply faceplate to lock the power supply in place.
7. For a 4-slot device only, use the screwdriver to secure the two screws on either side of the power supply faceplate.
8. For a 2400W DC power supply only, crimp the #4 AWG power supply wire in the power lugs.
9. For a 3000W DC power supply only, crimp the #2 AWG power supply wire in the power lugs.
10. Connect the AC power cord or DC power lugs to the power supply faceplate.
11. Connect the power to the AC or DC source.

    LEDs on the power supply faceplate show the status of the power supply with the following colors:

    - For a DC supply, the DC IN and DC OUT LEDs should be green, indicating the power supply is providing power to the device components.
    - For an AC supply, the AC OK and DC OK LEDs should be green, indicating the power supply is providing power to the device components (refer to the previous figure).
    - If the ALM LED is lit (amber), the power supply has failed.

    For information about troubleshooting this problem, refer to Management module LEDs on page 31.

Replacing fan assemblies

You can replace a fan or a fan control module while the router is powered on and running. The fans and fan control modules are located on the rear panel of the router.

NOTE
Fan trays are hot swappable. However, a hot-swap procedure should be completed within five minutes so the device will continue to function correctly without any fans. It is recommended that you disconnect the power supply from AC or DC power before installing or removing the fan tray.While fan assemblies are being replaced, and there is an increase or decrease in fan-speed due to that, syslogs or console messages are not generated.

Replacing fan assemblies in all MLXe-32 routers

This section describes how to replace fan assemblies in MLXe-32 routers.

CAUTION
Removal of ExtremeRouting MLX-32 rear fan modules allows access to bus bars and backplane. Avoid contact with these parts. There are hazardous energy levels at these locations.

An MLXe-32 router has ten fan assemblies located at the rear of the router. They are numbered as indicated in the following figure.

You can remove and replace a fan assembly while the router is powered on and running.

NOTE
To avoid overheating of the router, remove one fan assembly at a time, and replace it promptly. Wait for the LED on the fan assembly being replaced to turn green before replacing another fan assembly. Do not remove all fans from the device at once.

Before replacing a fan assembly, have the following items available:

- A new fan assembly, which you can order from Extreme Networks.
- A small flat-blade screwdriver
- An ESD wrist strap with a plug for connection to the ESD connector on the front of the device.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

Use the following steps to replace a fan assembly.

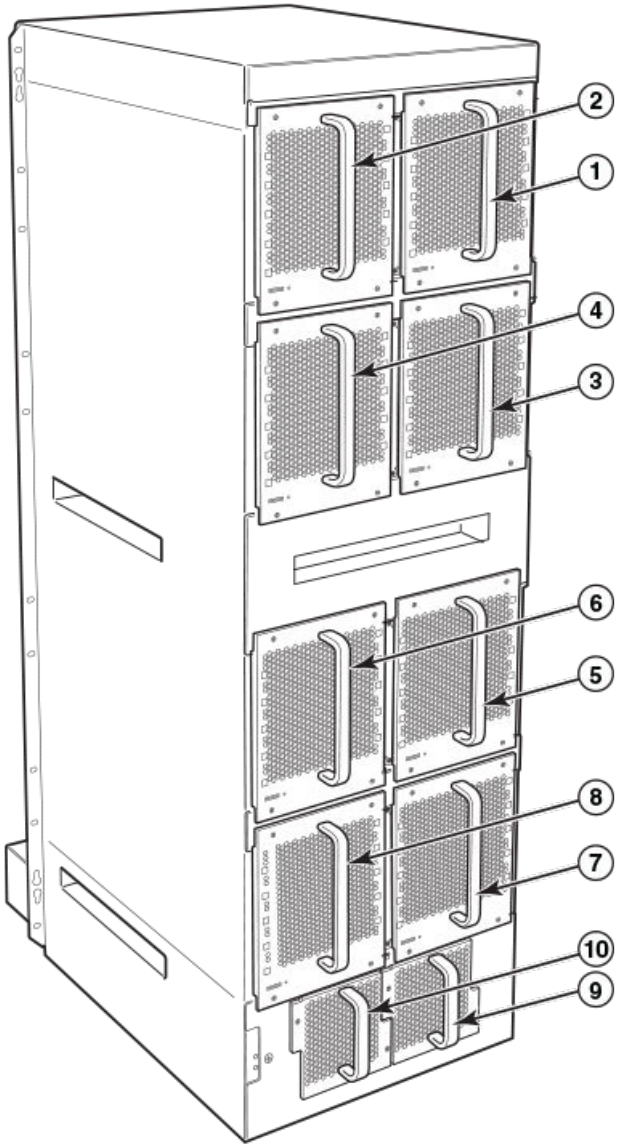
1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the router.
2. Using the screwdriver, remove the screws that secure the fan assembly faceplate to the rear of the router.

3. Remove the fan assembly by grasping the handle on the faceplate and pulling the assembly toward you as shown in Replacing the rear fan assemblies in 16-slot routers on page 258. Pulling the fan assembly unseats the fan connector from the device.

DANGER
The ExtremeRouting MLX-32 fan assembly is heavy and will be off-balance as you remove it. Use both hands on the handle.

DANGER
Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

FIGURE 111 MLXe-32 router fan assemblies



1	Fan module 1	6	Fan module 6
2	Fan module 2	7	Fan module 7

3	Fan module 3	8	Fan module 8
4	Fan module 4	9	Fan module 9
5	Fan module 5	10	Fan module 10

4. Insert the new fan assembly into the fan slot and push the assembly in until the faceplate is flush with the router. Pushing the fan assembly in seats the fan connector in the router connector.
5. Secure the fan assembly to the router by replacing and tightening the four screws (on the upper eight fan assemblies) and the two screws (on the lower two fan assemblies).
6. Check the fan status LED in the lower left corner of the faceplate. It will light red momentarily when power is applied, then change to green when the fan comes up to speed.
7. Access the CLI, and enter the **show chassis** command to verify that the fan is operating normally.

Replacing fan assemblies in MLXe-16 routers

The MLXe-16 routers have two fan assemblies accessible from the rear of the router.

You can remove and replace a fan assembly while the router is powered on and running.

NOTE
To avoid overheating of the 16-slot router, remove one fan assembly at a time, and replace it promptly. Do not remove all fans from the device at once.

CAUTION
If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

To replace a fan assembly, you need the following:

- A new fan assembly, which you can order from Extreme Networks.
- A small flat-blade screwdriver.
- An ESD wrist strap with a plug for connection to the ESD connector on the router.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

Replacing the rear fan assemblies in 16-slot routers

The instructions for replacing the rear fan assemblies in the 16-slot router apply to both standard) and high-speed fan assemblies.

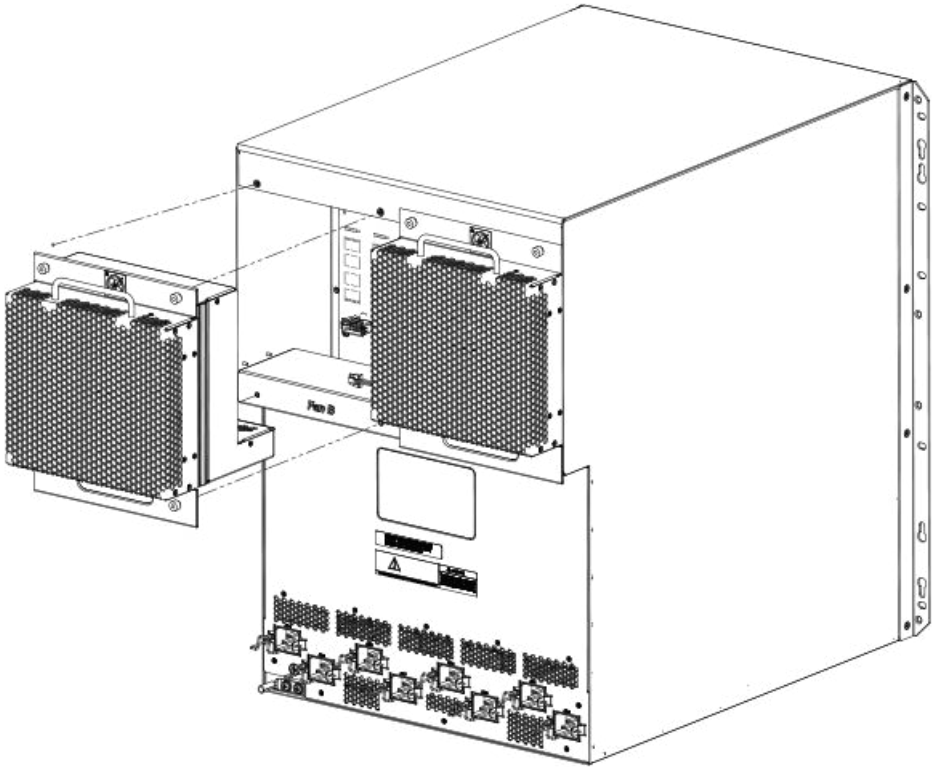
Perform these steps to replace a rear fan assembly.

1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the router.
2. Loosen the four captive screws that secure the fan assembly to the router.

3. Remove the fan by inserting your fingers underneath the fan assembly and pulling the assembly toward you as shown in the following figure. Pulling the fan assembly unseats the fan connector from the router connector.

   DANGER
   Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

   FIGURE 112 Replacing a fan assembly in a MLX-16 router



4. Insert the new fan assembly into the slot and push the assembly in until the faceplate is flush with the device. Pushing the assembly in seats the fan connector with the device connector.
5. Secure the fan assembly to the device by tightening the four captive screws.
6. Access the CLI, and enter the **show chassis** command to verify that both fans are operating normally.

Replacing the fan tray assembly in MLXe-4 and MLXe-8 routers

The fan tray assemblies for MLX Series 4-slot and 8-slot routers are accessible from the back of the device.

You can remove and replace a fan tray assembly while the router is powered on and running.

To replace a fan tray assembly, have these items available:

- A new fan tray assembly, which you can order from Extreme Networks.
- An ESD wrist strap with a plug for connection to the ESD connector on the router.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

NOTE
If you did not remove the extra shipment screws from the router during installation, you will not be able to remove the fan tray assembly. You will need to remove the router from the rack to remove the shipping screws, (refer to the installation chapter appropriate for your router model) before you can remove the fan tray assembly.

Follow these steps to replace fan tray assemblies in 4-slot routers.

1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the router.

2. To remove the fan tray assembly from the router, push down on the latch release with your thumb, grasp the handle, and pull it toward you as shown in the following two figures. Pulling the assembly unseats the fan tray assembly connector from a router connector.

   DANGER
   Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

   FIGURE 113 Replacing the fan assembly in an MLXe-4 router

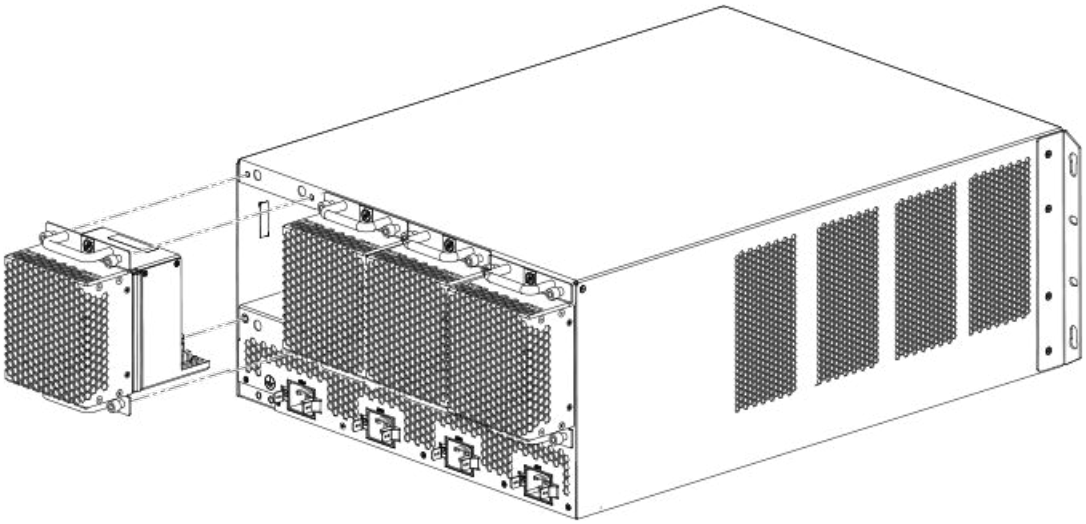
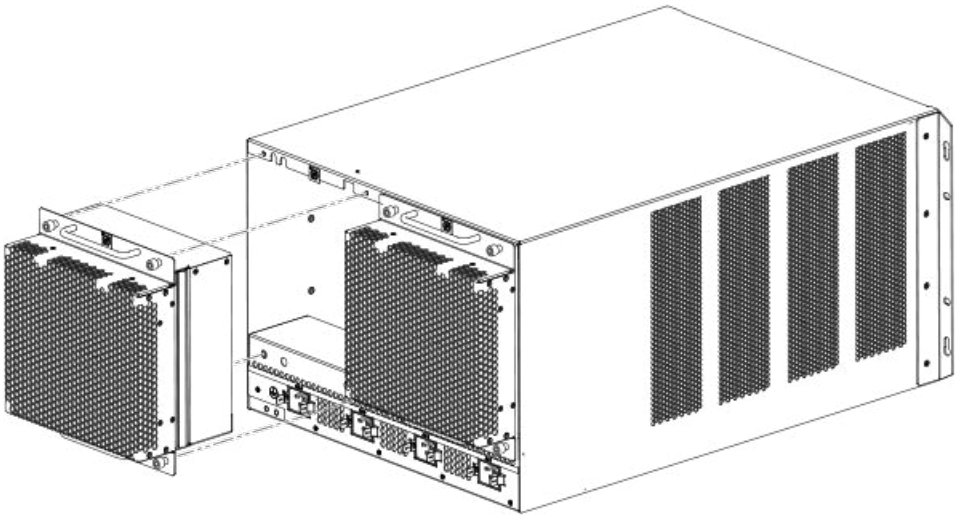


   FIGURE 114 Replacing the fan assembly in a MLXe-8 router



3. Insert the new fan assembly into the fan slot and push the enclosure in until the faceplate is flush with the router. Pushing the enclosure in seats the fan connector with the router connector.
4. Tighten the four captive screws to secure the fan to the router.
5. Access the CLI, and enter the **show chassis** command to verify that the fans are operating normally.

Replacing the air filters

It is strongly recommended that routers be installed in environments that have minimal dust and airborne contaminants. If routers are installed in environments where dust or other airborne contaminants may be present, air filters should be inspected and replaced as needed. Maintaining clean air filters ensures optimal airflow through the devices.

You can replace the air filters while a router is powered on and running. Before performing this task, have these items available:

- A 7/64 inch hex head screwdriver
- Replacement air filters, which you can order from Extreme Networks.

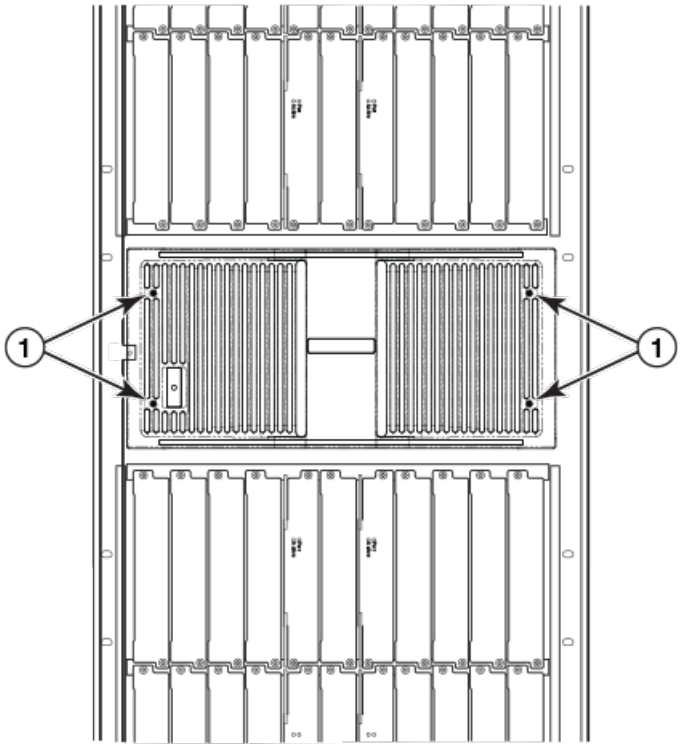
Replacing the air filters in 32-slot routers

The two air filters in 32-slot routers are located between the upper and lower card cages. To replace an air filter, perform these steps.

NOTE
Air filters for 32-slot routers are marked with a directional arrow to indicate proper alignment for the direction of airflow in the device. The upper filter should be inserted with the arrow pointing up, and the lower filter should be inserted with the arrow pointing down.

1. From the front of the router, remove the air inlet cover by unscrewing the four captive screws with a 7/64 inch hex head screwdriver, as shown in the following figure.

   FIGURE 115 32-slot router air inlet panel.

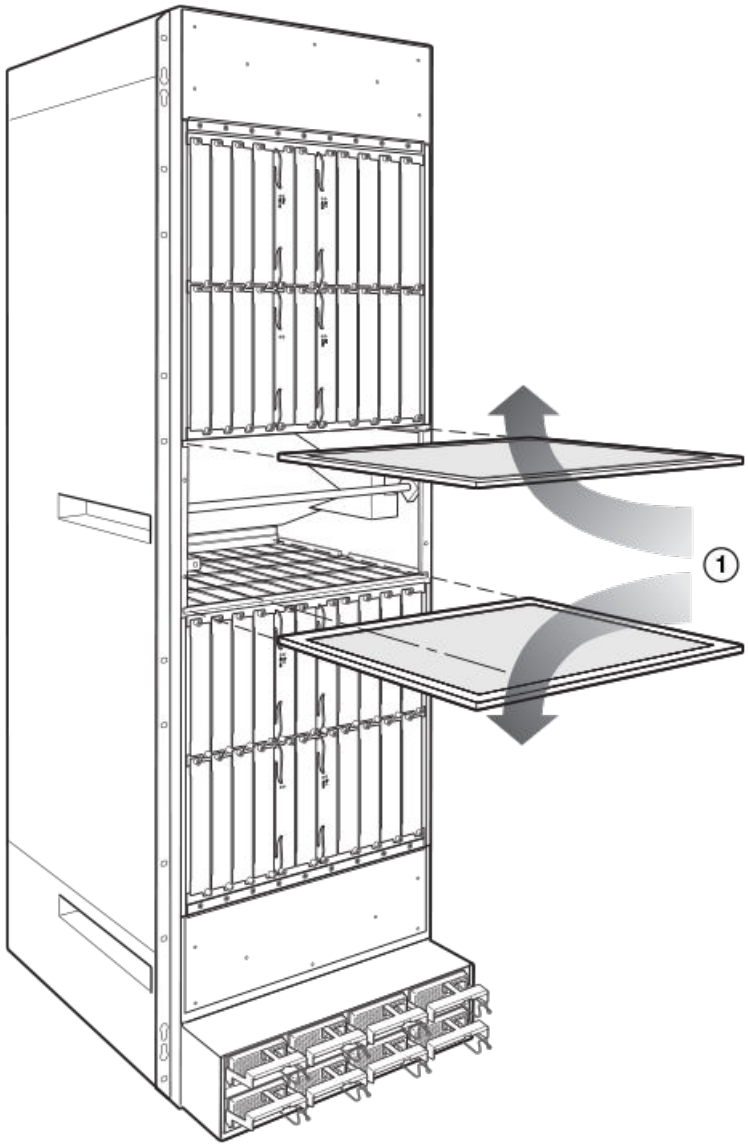


1	Captive screws

2. Remove the old air filter by pulling it straight out from the router, as shown in the following figure.

3. Insert a new filter, being careful that it aligns within the narrow channel.
4. Repeat steps 2 and 3 to replace the second filter.
5. Replace the air inlet cover and tighten the four captive screws to secure the air filter to the router.

FIGURE 116 Air filter removal and replacement for 32-slot routers



1	Direction of airflow in device

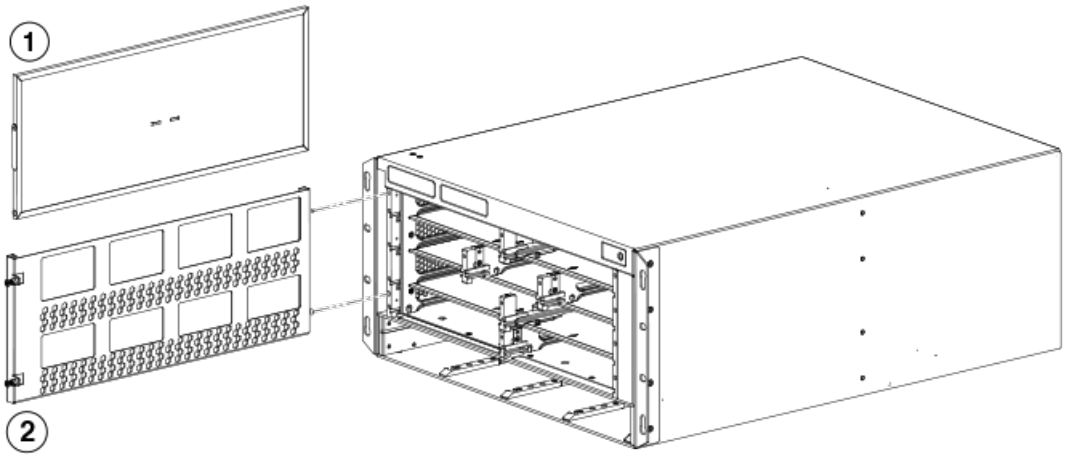
Replacing the air filter in MLX-4 and MLX-8 routers

Follow these steps to replace the air filter in MLX Series 4-slot and 8-slot routers.

1. Loosen the two screws in the front of the filter tray.

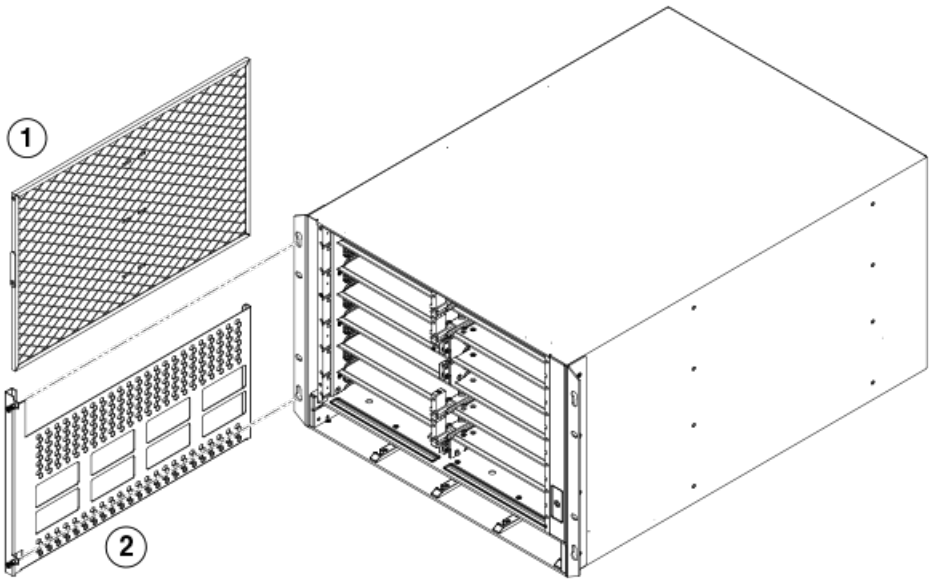
2. Pull the filter tray away from the router as shown in one of the following two figures.

FIGURE 117 Replacing an air filter in the MLX-4 router.



1	Air filter
2	Air filter tray

FIGURE 118 Air filter removal and replacement for the MLX-8 router.



1	Air filter
2	Air filter tray

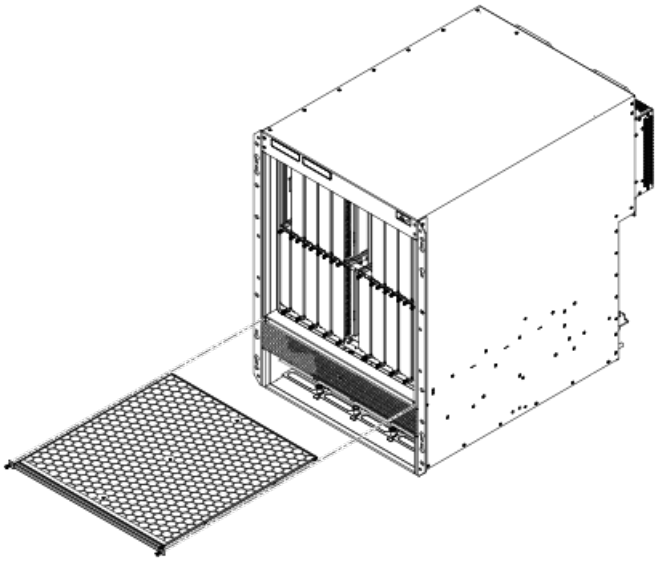
3. Remove the old air filter from the tray and discard it.
4. Insert the replacement air filter into the air filter tray.
5. Replace the filter tray in the router and tighten the two screws.

Replacing the air filter in MLX-16 routers

Follow these steps to replace the air filter in a MLX Series 16-slot router.

1. Loosen the two screws in the front of the filter.
2. Pull the filter out of the router as shown in the following figure.

FIGURE 119 Replacing the air filter in the MLX-16 routers



3. Remove the old filter from the chassis and discard the used filter.
4. Insert a new air filter into the filter slot and tighten the two screws.

Installing upward deflectors on fan assemblies

Before beginning this procedure, verify that you have the correct number of upward deflectors (part number 80-1004745-01). You can install up to eight deflectors on each router. You can remove each fan assembly while the router is running; however, you must not remove more than one fan assembly at any time to prevent the router from overheating.

NOTE
If the router is not receiving power, you can remove more than one fan assembly at a time.

It will take about one hour to complete this procedure for each MLXe-32 router.

The following items are required for this procedure:

- Phillips screwdriver
- Small flathead screwdriver
- ESD wrist strap

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

Removing a fan assembly from the chassis

To remove a fan assembly from the chassis that is receiving power, complete the following steps:

1. Put on the ESD wrist strap and ground yourself by inserting the plug into the ESD connector on the router.
2. Depending on your router model (MLXe-32) use the appropriate screwdriver to remove the screws that secure the fan assembly faceplate to the rear of the router.

   DANGER
   The ExtremeRouting MLX-32 fan assembly is heavy and will be off-balance as you remove it. Use both hands on the handle.

   DANGER
   Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

   CAUTION
   Removal of ExtremeRouting MLX-32 rear fan modules allows access to bus bars and backplane. Avoid contact with these parts. There are hazardous energy levels at these locations.

3. Remove the fan assembly by grasping the handle on the faceplate and pulling the fan assembly toward you. Pulling the fan assembly unseats the fan connector from the router.

Attaching the upward deflector

The upward deflector is placed between the fan assembly handle and the fan assembly faceplate. To install the upward deflector to each fan assembly, complete the following steps:

1. Using a Phillips screwdriver, detach the fan assembly faceplate by removing the three screws from each side of the fan assembly. Refer to Replacing the fan tray assembly in MLXe-4 and MLXe-8 routers on page 259.

2. If present, remove and discard the tape that stabilizes louvers in some fan assembly models. When present, the tape is located on the right and left sides of the fan assembly.

FIGURE 120 Removing the fan assembly faceplate

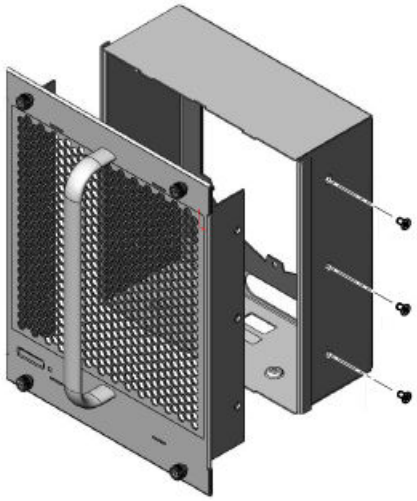
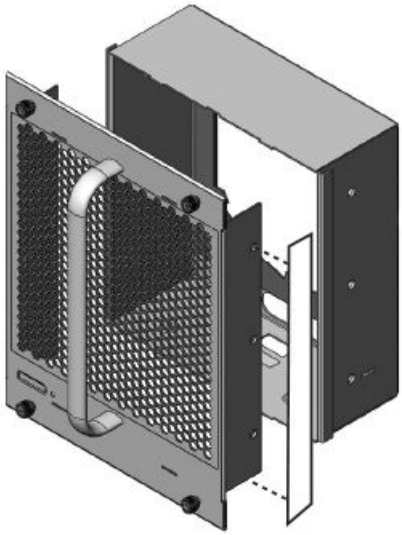


FIGURE 121 Removing tape from the fan assembly



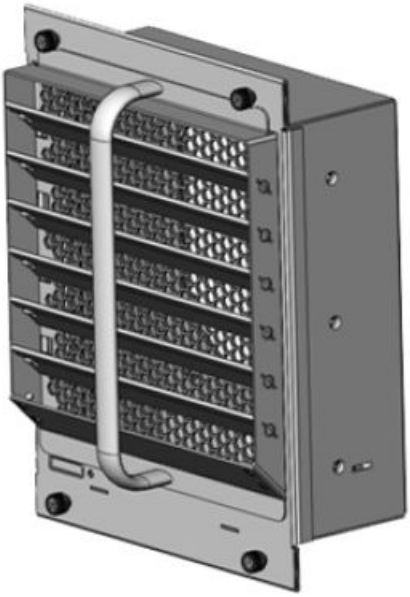
3. Remove the fan assembly handle by detaching the two screws from the inside of the fan assembly faceplate using a Phillips screwdriver, as shown in the following figure.

   FIGURE 122 Handle removal

4. Orient the upward deflector on the fan assembly faceplate so that the exhaust will flow upward and the holes in the upward deflector align with the holes where the screws secure the handle to the fan assembly faceplate. Refer to the previous figure.

5. Place the handle over the upward deflector aligning the handle with the screw holes, and secure the handle to the upward deflector and fan assembly faceplate with the two screws, as shown in the following figure.

   FIGURE 123 Upward deflector oriented correctly between the handle and fan assembly faceplate



6. Re-attach the fan assembly faceplate to the fan assembly by securing three screws on each side.

   NOTE
   Replacing the tape is not required.

Reinstalling the modified fan assembly in the chassis

To reinstall the modified fan assembly, complete the following steps:

1. Insert the modified fan assembly into the fan slot and push the assembly in until the fan assembly faceplate is flush with the chassis. Pushing the fan assembly in seats the fan connector in the router connector.
2. Secure the fan assembly to the router by replacing and tightening the four screws.
3. Check the fan status LED in the lower left corner of the faceplate. It will glow red momentarily when power is applied, and then it will change to green when the fan comes up to speed.
4. To verify that the fan is operating correctly, access the CLI and enter the **show chassis** command.

Hardware Specifications

- Hardware specifications for ExtremeRouting MLX Series routers....271
- Port specifications for all router models....275

Hardware specifications for ExtremeRouting MLX Series routers

The following sections describe hardware specifications for MLX Series routers.

Power specifications

The following power supply frequency requirements apply to MLXe-4, MLXe-8, and MLXe-16 routers:

- AC Input Rating: 100 to 240V, 50/60 Hz, 16.0 A maximum per power supply
  - 1200W Power Output for 1200W PSU (100-240V)
  - 1200W Power Output for 1800W PSU (100-180V)
  - 1800W Power Output for 1800W PSU (180-240V)
- AC Operating Voltage Range: 90 to 264V, 50/60 Hz
  - Inrush current <60A peak for any initial current surge or spike of 10mS or less at either cold or warm start. Any additional inrush current surges or spikes in the form of AC cycles or multiple AC cycles greater than 10mS and less than 150mS will be <25A peak.
- DC Input Rating: -48V
  - 40A maximum per power supply (1200W PSU)
  - 60A maximum per power supply (1800W PSU)
- DC Operating Range: -40 to -60V
  - Inrush current <80A peak for any initial current surge or spike of 10mS or less at either cold or warm start.

The following power supply frequency requirements apply to the MLX-32 routers:

- AC Input Rating: 200 to 240V, 50/60 Hz, 16.0 A maximum per power supply
- AC Operating Voltage Range: 180 to 264V
  - Inrush current <60A peak for any initial current surge or spike of 10mS or less at either cold or warm start. Any additional inrush current surges or spikes in the form of AC cycles or multiple AC cycles greater than 10mS and less than 150mS will be <25A peak.
- DC Input Rating: -48V
  - 75A maximum per power supply (2400W PSU)
  - 80A maximum per power supply (3000W PSU)
- DC Operating Range: -40 to -60V
  - Inrush current <70A peak for any initial current surge or spike of 10mS or less at either cold or warm start.

NOTE

3000W power supplies do not support low line AC Input Voltage.

The following table lists power consumption, in watts, for MLX Series router components.

TABLE 48 Maximum power consumption for MLX Series router components

Component	Maximum power consumption, in watts
Management modules	
MR Management modules (MLXe-4, MLXe-8, and MLXe-16 routers)	30W
MR Management module (MLXe-32 routers)	35W
MR2 management module (BR-MLX-32-MR2-M for MLX Series routers)	45W
MR2 management module (BR-MLX-MR2-M for MLX Series routers)	40W
Switch fabric modules	
NI-X-SF3 switch fabric module	53W
NI-X-SF1 switch fabric module	19W
NI-X-32-SF switch fabric module	60W
High speed switch fabric modules	
NI-X-4-HSF switch fabric module (MLXe-4 routers)	19W
NI-X-16-8-HSF switch fabric module (MLXe-8 and MLXe-16 routers)	53W
NI-X-32-HSF switch fabric module (MLXe-32 routers)	60W
Interface modules	
1-port 100 Gbps Ethernet interface module	485W
2-port 100 Gbps Ethernet interface module	640W
2-port 10 Gbps Ethernet interface module (XMR routers)	
2-port 10 Gbps Ethernet interface module with fiber-optic transceivers (MLX Series routers)	150W
4-port 10 Gbps Ethernet interface module with fiber-optic transceivers (MLX Series routers)	225W
4-port 40-GbE Ethernet module (M)	320W
8-port 10 Gbps SFPP module (M)	246W
8-port 10 Gbps SFPP interface module (D)	246W
8-port 10 Gbps interface module (X)	270W
20-port Gbps Ethernet fiber Interface with fiber-optic transceivers (MLX Series routers)	175W
20-port Gbps Ethernet copper Interface module	146W
24-port 1 Gbps Ethernet copper RJ45 interface module	160W
24-port 1 Gbps Ethernet fiber interface module	160W
24-port 10 Gbps Ethernet interface module	320W
48-port Gbps Ethernet with MRJ-21 interface	260W

The following table lists power consumption information for MLX Series routers with all base components installed, and with only the specified interface modules installed.

TABLE 49 MLX Series router power consumption values

Model	@100 VAC			@200 VAC			@-48VDC			Minimum number of 1200W power supplies needed	Minimum number of 1800W power supplies needed	Minimum number of 2400W power supplies needed	Minimum number of 3000W power supplies needed
Amps	Watts	BTU/hr	Amps	Watts	BTU/hr	Amps	Watts	BTU/hr					
MAXIMUM PER MLX (using 8x10G-D, 8x10G-M, 4x10G, 2x10G, 1G modules only)													
MLX-4	17	1730	5905	9	1730	5905	36	1730	5905	2	1		
MLX-8	34	3356	11453	17	3356	11453	70	3356	11453	3	2		
MLX-16	57	5698	19446	28	5698	19446	119	5698	19446	4	3		
MLX-32	N/A	N/A	N/A	57	11414	38958	238	11414	38958			4	4
MAXIMUM PER MLX (any module)													
MLX-4	21	2083	7108	10	2083	7108	43	2083	7108	2	1		
MLX-8	41	4060	13858	20	4060	13858	85	4060	13858	3	2		
MLX-16	71	7107	24255	36	7107	24255	148	7107	24255	5	4		
MLX-32	N/A	N/A	N/A	71	14232	48575	297	14232	48575			5	4

Physical dimensions

The following table provides the physical dimensions for MLX Series routers.

TABLE 50 MLX Series routers physical dimensions

Router model	Height	Width	Depth	Depth with Fan FRU	Weight (empty)	Weight (fully loaded)
MLX Series-4	22.13 cm (8.714 in.)	43.69 cm (17.20 in.)	58.42 cm (23.0 in.)	63.5 cm (25.0 in.)	27.40 kg (60.4 lbs)	52.84 kg (116.5 lbs.)
MLX Series-8	31.01 cm (12.21 in.)	43.69 cm (17.20 in.)	60.96 cm (24.0 in.)	66.04 cm (26.0 in.)	35.47 kg (78.2 lbs.)	77.72 kg (171.35 lbs.)
MLX Series-16	62.15 cm (24.47 in.)	44.32 cm (17.45 in.)	61.42 cm (24.18 in.)	66.50 cm (26.18 in.)	41.66 kg (91.95 lbs.)	159.39 kg (351.4 lbs)
MLX Series-32	146.58 cm (57.71 in.)	44.32 cm (17.45 in.)	68.30 cm (26.9 in.)	68.58 cm (27.0 in.)	128.68 kg (283.7 lbs.)	228.97 kg (504.8 lbs)

The following table provides the physical dimensions for MLX Series router interface modules.

TABLE 51 MLX Series router interface modules physical dimensions

Interface module model	Height	Width	Depth	Depth with Fan FRU	Weight (empty)	Weight (fully loaded)
BR-MLX-40GX4-M	4.166 cm (1.46 in.)	18.796 cm (7.40 in.)	40.64 cm (16.0 in.)	NA	NA	4 kg (9.85 lbs)

Operating environment

The following table provides the operating environment specifications for MLX Series routers.

TABLE 52 MLX Series router operating environment

Operating temperature	Relative humidity	Operating altitude
(0° - 40°C) 32° - 104°F	5 to 90%, at (40°C) 104°F, non-condensing	(0 - 3km) 0 - 10,000 ft

Storage environment

The following table provides the storage environment specifications for the MLX Series routers.

TABLE 53 MLX Series router storage environment

Storage temperature	Storage humidity	Storage altitude
(-25° - 70°C) -13° - 158°F	95% maximum relative humidity, non-condensing	(0 - 4500 meters) 0 - 15,000 ft

Safety agency approvals

- CAN/CSA-C22.2 No. 60950-1-07/UL60950-1 - Second Edition, Safety of Information Technology Equipment
- EN 60825-1 Safety of Laser Products - Part 1: Equipment Classification, Requirements and User's Guide
- EN 60825-2 Safety of Laser Products - Part 2: Safety of Optical Fibre Communications Systems
- EN 60950-1:2006\IEC 60950-1:2005, Second Edition, Safety of Information Technology Equipment

Electromagnetic approvals

- FCC Part 15, Subpart B (Class A)
- EN 55022 (CE mark) (Class A)
- EN 55024 (CE mark) (Immunity) for Information Technology Equipment
- ICES-003 (Canada) (Class A)
- AS/NZ 55022 (Australia) (Class A)
- VCCI (Japan) (Class A)
- EN 61000-3-2
- EN 61000-3-3
- EN 61000-6-1

Port specifications for all router models

This section describes port specifications for all router models.

2x100GbE CFP2 Dynamic Port Configuration

The dynamic port configuration is shown for the 2x100GbE CFP2 based high density blade chassis.

Dynamic port configuration for the 20x10/1GbE based high density blade chassis is shown in the following table.

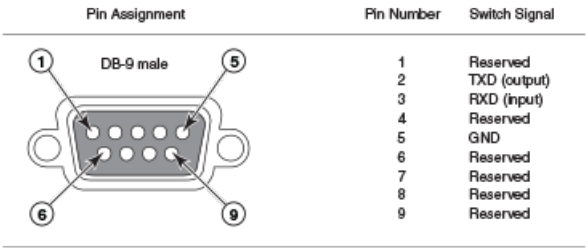
TABLE 54 20x10/1GbE Module Dynamic Port Configuration

# Ports	Line Speed	SFP Type	Configuration Status	Port Speed Status
20	1GbE	SFP	1GbE	Supported
	10GbE	SFP+	10GbE	Supported
	10GbE	SFP	10GbE	Not Supported
	1GbE	SFP+	1GbE	Not Supported
	10GbE	SFP+	1GbE	Not Supported

Console port pin assignments

The console port is a standard male DB-9 connector, as shown in the following figure. For information about how you can use this port, refer to Console port on page 31.

FIGURE 124 Console port pin and signaling details



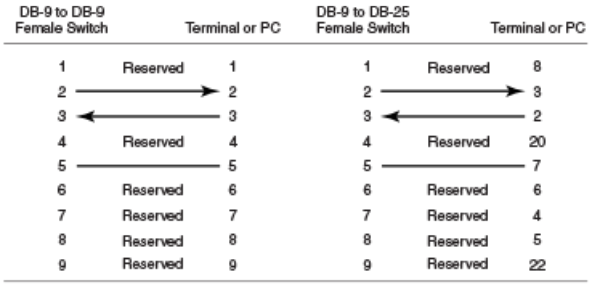
1	Reserved	6	Reserved
2	TXD (output)	7	Reserved
3	RXD (input)	8	Reserved
4	Reserved	9	Reserved
5	GND		

Most PC serial ports require a cable with a female DB-9 connector. Terminal connections will vary, requiring a cable with either a DB-9 or DB-25 connector, male or female.

Serial cable options between the router and a PC or terminal are shown in the following table.

> **NOTE**
> As shown in the figures in this section, some wires should not be connected. If you connect wires that are labeled "Reserved", you may experience unexpected results with some terminals.

FIGURE 125 Console port pin assignments with connection options to a terminal or PC



Management port pin assignments

The management port is an RJ45 UTP connector. The following table describes the pin assignments for this connector. For information about how you can use this port, refer to 10/100/1000 Ethernet port on page 31.

TABLE 55 Management port pin assignments

Pin number	MDI-X ports
1	TD+
2	TD-
3	RD+
4	Not used (10BaseT)CMT (100BaseTX)
5	Not used (10BaseT)CMT (100BaseTX)
6	RD-
7	Not used (10BaseT)CMT (100BaseTX)
8	Not used (10BaseT)CMT (100BaseTX)

ExtremeRouting MLX Series Chassis Bundles

The following tables describe the ExtremeRouting MLX Series chassis bundles and their components.

TABLE 56 MLXe-4 chassis bundles

Part number	Hardware
BR-MLXE-4-AC	Bundle contents: • 1 MLX-4 chassis • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1200W AC power supply(NI-X-ACPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-4-DC	Bundle contents: • 1 MLX-4 chassis • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1200W DC power supply(NI-X-DCPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-4-MR-M-AC	Bundle contents: • 1 MLXe-4 AC chassis • 1 MR management module(NI-MLX-MR) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1200W AC power supply(NI-X-ACPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR-M-DC	Bundle contents: • 1 MLXe-4 DC chassis • 1 MR management module(NI-MLX-MR) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1200W DC power supply(NI-X-DCPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR-X-AC	Bundle contents: • 1 MLXe-4 AC chassis • 1 MR management module(NI-XMR-MR) • 2 high speed switch fabric modules(NI-X-4-HSF)

TABLE 56 MLXe-4 chassis bundles (continued)

Part number	Hardware
	• 1 1200W AC power supply(NI-X-ACPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter (BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR-X-DC	Bundle contents: • 1 MLXe-4 AC chassis • 1 MR management module (NI-XMR-MR) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1200W DC power supply(NI-X-DCPWR) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR2-M-AC	Bundle contents: • 1 MLXe-4 AC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1800W AC power supply(BR-MLXE-ACPWR-1800) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter (BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR2-M-DC	Bundle contents: • 1 MLXe-4 DC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1800W DC power supply(BR-MLXE-DCPWR-1800) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR2-X-AC	Bundle contents: • 1 MLXe-4 AC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1800W AC power supply(BR-MLXE-ACPWR-1800) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.
BR-MLXE-4-MR2-X-DC	Bundle contents: • 1 MLXe-4 DC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 2 high speed switch fabric modules(NI-X-4-HSF) • 1 1800W DC power supply(BR-MLXE-DCPWR-1800) • 4 exhaust fan assembly kits(BR-MLXE-4-FAN) • 1 air filter(BR-MLXE-4-FLTR) Power cord is not included.

TABLE 57 MLX-8 chassis bundles

Part number	Hardware
BR-MLXE-8-AC	Bundle contents: • 1 MLX-8 chassis • 2 high speed switch fabric modules(NI-X-16-8-HSF) • 2 1200W AC power supplies(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter (BR-MLXE-8-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-8-DC	Bundle contents: • 1 MLX-8 chassis • 2 high speed switch fabric modules(NI-X-16-8-HSF) • 2 1200W DC power supplies(NI-X-DCPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-8-MR-M-AC	Bundle contents: • 1 MLX-8 AC chassis • 1 MR management module(NI-MLX-MR) • 2 high speed switch fabric modules(NI-X-16-8-HSF) • 2 1200W AC power supply(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR-M-DC	Bundle contents: • 1 MLXe-8 DC chassis • 1 MR management module (NI-MLX-MR) • 2 high speed switch fabric modules(NI-X-16-8-HSF) • 2 1200W DC power supply(NI-X-DCPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR-X-AC	Bundle contents: • 1 MLXe-8 AC chassis • 1 MR management module(NI-XMR-MR) • 2 high speed switch fabric modules(NI-X-16-8-HSF) • 2 1200W AC power supply (NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR-X-DC	Bundle contents: • 1 MLXe-8 DC chassis • 1 MR management module(NI-XMR-MR) • 2 high speed switch fabric modules(NI-X-16-8-HSF)

TABLE 57 MLX-8 chassis bundles (continued)

Part number	Hardware
	• 2 1200W DC power supply(NI-X-DCPWR) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR2-M-AC	Bundle contents: • 1 MLXe-8 AC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 2 high speed switch fabric modules(NI-X-4-HSF) • 2 1800W AC power supplies(BR-MLXE-ACPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR2-M-DC	Bundle contents: • 1 MLXe-8 DC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 2 high speed switch fabric modules(NI-X-4-HSF) • 2 1800W DC power supplies(BR-MLXE-DCPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR2-X-AC	Bundle contents: • 1 MLXe-8 AC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 2 high speed switch fabric modules(NI-X-4-HSF) • 2 1800W AC power supplies(BR-MLXE-ACPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter(BR-MLXE-8-FLTR) Power cord is not included.
BR-MLXE-8-MR2-X-DC	Bundle contents: • 1 MLXe-8 DC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 2 high speed switch fabric modules(NI-X-4-HSF) • 2 1800W DC power supplies(BR-MLXE-DCPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-8-FAN) • 1 air filter (BR-MLXE-8-FLTR) Power cord is not included.

TABLE 58 MLX Series-16 chassis bundles

Part number	Hardware
BR-MLXE-16-AC	Bundle contents: • 1 MLX-16 chassis • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W AC power supplies(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN)

TABLE 58 MLX Series-16 chassis bundles (continued)

Part number	Hardware
	• 1 air filter(BR-MLXE-16-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-16-DC	Bundle contents: • 1 MLX-16 chassis • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W DC power supplies(NI-X-DCPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Management modules must be ordered separately. Power cord is not included.
BR-MLXE-16-MR-M-AC	Bundle contents: • 1 MLXe-16 AC chassis • 1 MR management module(NI-MLX-MR) • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W AC power supply(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR-M-DC	Bundle contents: • 1 MLXe-16 DC chassis • 1 MR management module (NI-MLX-MR) • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W DC power supply(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR-X-AC	Bundle contents: • 1 MLXe-16 AC chassis • 1 MR management module(NI-XMR-MR) • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W AC power supply(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter (BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR-X-DC	Bundle contents: • 1 MLXe-16 DC chassis • 1 MR management module(NI-XMR-MR) • 3 high speed switch fabric modules(NI-X-16-8-HSF) • 4 1200W DC power supply(NI-X-ACPWR) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.

TABLE 58 MLX Series-16 chassis bundles (continued)

Part number	Hardware
BR-MLXE-16-MR2-M-AC	Bundle contents: • 1 MLXe-16 AC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 3 high speed switch fabric modules(NI-X-4-HSF) • 4 1800W AC power supplies(BR-MLXE-ACPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter (BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR2-M-DC	Bundle contents: • 1 MLXe-16 DC chassis • 1 MR2 (M) management module(BR-MLX-MR2-M) • 3 high speed switch fabric modules(NI-X-4-HSF) • 4 1800W DC power supplies(BR-MLXE-DCPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR2-X-AC	Bundle contents: • 1 MLXe-16 AC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 3 high speed switch fabric modules(NI-X-4-HSF) • 4 1800W AC power supplies(BR-MLXE-ACPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.
BR-MLXE-16-MR2-X-DC	Bundle contents: • 1 MLXe-16 DC chassis • 1 MR2 (X) management module(BR-MLX-MR2-X) • 3 high speed switch fabric modules(NI-X-4-HSF) • 4 1800W DC power supplies(BR-MLXE-DCPWR-1800) • 2 exhaust fan assembly kits(BR-MLXE-16-FAN) • 1 air filter(BR-MLXE-16-FLTR) Power cord is not included.

TABLE 59 MLX Series chassis spares

Part Number	Hardware	Installation guide
BR-MLXE-4-S	1 MLX-4 spare chassis	*ExtremeRouting MLX Series and ExtremeRouting XMR/MLX Hardware Installation Guides*
BR-MLXE-8-S	1 MLX-8 spare chassis	*ExtremeRouting MLX Series and ExtremeRouting XMR/MLX Hardware Installation Guides*
BR-MLXE-16-S	1 MLX-16 spare chassis	*ExtremeRouting MLX Series and ExtremeRouting XMR/MLX Hardware Installation Guides*

TABLE 59 MLX Series chassis spares (continued)

Part Number	Hardware	Installation guide
BR-MLXE-32-S	1 MLX-32 spare chassis	*ExtremeRouting MLX Series and ExtremeRouting XMR/MLX Hardware Installation Guides*

TABLE 60 MLX-32 chassis bundles

Part number	Hardware
BR-MLXE-32-AC	Bundle contents: • 1 MLX-32 chassis • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W AC power supplies(NIBI-32-ACPWR-A) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Management modules must be ordered separately. Power cord is not included.
BR-MLXE-32-DC	Bundle contents: • 1 MLX-32 chassis • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W DC power supplies(NIBI-32-DCPWR) • 2 power supply fans (NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Management modules must be ordered separately. Power cord is not included.
BR-MLXE-32-MR-M-AC	Bundle contents: • 1 MLXe-32 AC chassis • 1 MR management module(NI-MLX-32-MR) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W AC power supplies(NIBI-32-ACPWR-A) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR-M-DC	Bundle contents: • 1 MLXe-32 DC chassis • 1 MR management module(NI-MLX-32-MR) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W DC power supplies(NIBI-32-DCPWR) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits (BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR)

TABLE 60 MLX-32 chassis bundles (continued)

Part number	Hardware
	• Cable management system Power cord is not included.
BR-MLXE-32-MR-X-AC	Bundle contents: • 1 MLXe-32 AC chassis • 1 MR management module(BR-MLX-32-MR) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W AC power supplies(NIBI-32-ACPWR-A) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR-X-DC	Bundle contents: • 1 MLXe-32 DC chassis • 1 MR management module(BR-MLX-32-MR) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 2400W DC power supplies(NIBI-32-DCPWR) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR2-M-AC	Bundle contents: • 1 MLXe-32 AC chassis • 1 MR2 (M) management module(BR-MLX-32-MR2-M) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 3000W AC power supplies(BR-MLXE-32-ACPWR-3000) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR2-M-DC	Bundle contents: • 1 MLXe-32 DC chassis • 1 MR2 (M) management module(BR-MLX-32-MR2-M) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 3000W DC power supplies(BR-MLXE-32-DCPWR-3000) • 2 power supply fans (NIBI-32-PSFAN) • 8 exhaust fan assembly kits (BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR2-X-AC	Bundle contents: • 1 MLXe-32 AC chassis

TABLE 60 MLX-32 chassis bundles (continued)

Part number	Hardware
	• 1 MR2 (X) management module(BR-MLX-32-MR2-X) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 3000W AC power supplies(BR-MLXE-32-ACPWR-3000) • 2 power supply fans (NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters(BR-MLXE-32-FLTR) • Cable management system Power cord is not included.
BR-MLXE-32-MR2-X-DC	Bundle contents: • 1 MLXe-32 DC chassis • 1 MR2 (X) management module(BR-MLX-32-MR2-X) • 7 high speed switch fabric modules(NI-X-32-HSF) • 4 3000W DC power supplies(BR-MLXE-32-DCPWR-3000) • 2 power supply fans(NIBI-32-PSFAN) • 8 exhaust fan assembly kits(BR-MLXE-32-FAN) • 2 air filters (BR-MLXE-32-FLTR) • Cable management system Power cord is not included.

Regulatory Statements

- BSMI statement (Taiwan) 287
- Canadian requirements 287
- China CC statement 288
- Europe and Australia (CISPR 22 Class A Warning) 288
- FCC warning (US only) 289
- Germany 289
- KCC statement (Republic of Korea) 289
- VCCI statement 290
- Japan power cord 290
- EMC, safety, and environmental regulatory compliance information 290

BSMI statement (Taiwan)

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，
在這種情況下，使用者會被要求採取某些適當的對策。

Warning:

This is Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Canadian requirements

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations, ICES-003 Class A.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

China CC statement

China-CCC Warning statements

在维修的时候一定要断开所有电源 (English translation"disconnect all power sources before service")

For non tropical use:

安全说明和标记	汉文	"仅适用于非热带气候条件下安全使用。"
	藏文	[illegible]
	蒙古文	"ཚ་བའི་ས་ཁུལ་གྱི་གནམ་གཤིས་མིན་པའི་ས་ཁུལ་ཁོ་ནར་ཉེན་མེད་བེད་སྤྱོད་བྱས་འཐུས།"
	壮文	Dan hab yungh youq gij dienheiq diuzgen mbouj dwg diegndat haenx ancienz sawjyungh.
	维文	غەيرى ئىسسىق بەلباغ ھاۋا كىلىماتى شارائىتىدىلا بىخەتەر ئىشلەتكىلى بولىدۇ

For altitude 2000 meter and below:

安全说明和标记	汉文	仅适用于海拔2000m以下地区安全使用。
	藏文	《2000m [illegible]
	蒙古文	"རྒྱ་མཚོའི་ངོས་ལས་མཐོ་ཚད་སྨི2000མན་གྱི་ས་ཁུལ་ཁོ་ནར་ཉེན་མེད་བེད་སྤྱོད་བྱས་འཐུས།"
	壮文	Dan hab yungh youq gij digih haijbaz 2000m doxroengz haenx ancienz sawjyungh.
	维文	دېڭىز يۈزىدىن 2000 مېتر تۆۋەن رايونلاردىلا بىخەتەر ئىشلەتكىلى بولىدۇ

Warning for Class A:

声 明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

English translation of above statement

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Europe and Australia (CISPR 22 Class A Warning)

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC warning (US only)

This equipment has been tested and complies with the limits for a Class A computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

Germany

For MLX Series-32 routers:

Machine noise information regulation - 3. GPSGV, the highest sound pressure level value is 88.4 dB(A) in accordance with EN ISO 7779.

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 88.4 dB(A) gemäss EN ISO 7779.

For MLX Series-16 routers:

Machine noise information regulation - 3. GPSGV, the highest sound pressure level value is 98.0 dB(A) in accordance with EN ISO 7779.

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 98.0 dB(A) gemäss EN ISO 7779.

For MLX Series-8 routers:

Machine noise information regulation - 3. GPSGV, the highest sound pressure level value is 87.4 dB(A) in accordance with EN ISO 7779.

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 87.4 dB(A) gemäss EN ISO 7779.

For MLX Series-4 routers:

Machine noise information regulation - 3. GPSGV, the highest sound pressure level value is 86.0 dB(A) in accordance with EN ISO 7779.

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 86.0 dB(A) gemäss EN ISO 7779.

KCC statement (Republic of Korea)

A급 기기 (업무용 방송통신기기): 이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자
또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Class A device (Broadcasting Communication Device for Office Use): This device obtained EMC registration for office use (Class A), and may be used in places other than home. Sellers and/or users need to take note of this.

VCCI statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance might arise. When such trouble occurs, the user might be required to take corrective actions.

Japan power cord

注意 – 添付の電源コードを他の装置や用途に使用しない
添付の電源コードは本装置に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないでください。火災や感電の原因となる恐れがあります。

English translation of above statement

ATTENTION: Never use the power cord packed with your equipment for other products.

EMC, safety, and environmental regulatory compliance information

Regulatory compliance (EMC)

- FCC Part 15, Subpart B (Class A)
- EN 55022 (CE mark) (Class A)
- EN 55024 (CE mark) (Immunity) for Information Technology Equipment
- ICES-003 (Canada) (Class A)
- AS/NZ 55022 (Australia) (Class A)
- VCCI (Japan) (Class A)
- EN 61000-3-2
- EN 61000-3-3

- EN 61000-6-1

Regulatory compliance (safety)

- CAN/CSA-C22.2 No. 60950/UL 60950
- EN 60825 Safety of Laser Products
- EN 60950/IEC 60950 Safety of Information Technology Equipment

Regulatory compliance (environmental)

- 2014/35/EU and 2014/30/EU
- 2011/65/EU - Restriction of the use of certain hazardous substance in electrical and electronic equipment (EU RoHS).
- 2012/19/EU - Waste electrical and electronic equipment (EU WEEE).
- 94/62/EC - packaging and packaging waste (EU).
- 2006/66/EC - batteries and accumulators and waste batteries and accumulators (EU battery directive).
- 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (EU REACH).
- Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 - U.S. Conflict Minerals.
- 30/2011/TT-BCT - Vietnam circular.
- SJ/T 11363-2006 Requirements for Concentration Limits for Certain Hazardous Substances in EIPs (China).
- SJ/T 11364-2006 Marking for the Control of Pollution Caused by EIPs (China).

Caution and Danger Notices

- Cautions....293
- Danger Notices....301

Cautions

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Ein Vorsichthinweis warnt Sie vor potenziellen Personengefahren oder Beschädigung der Hardware, Firmware, Software oder auch vor einem möglichen Datenverlust

Un message de mise en garde vous alerte sur des situations pouvant présenter un risque potentiel de dommages corporels ou de dommages matériels, logiciels ou de perte de données.

Un mensaje de precaución le alerta de situaciones que pueden resultar peligrosas para usted o causar daños en el hardware, el firmware, el software o los datos.

General cautions

CAUTION
Do not install the device in an environment where the operating ambient temperature might exceed 40°C (104°F).

VORSICHT	Das Gerät darf nicht in einer Umgebung mit einer Umgebungsbetriebstemperatur von über 40°C (104°F) installiert werden.
MISE EN GARDE	N'installez pas le dispositif dans un environnement où la température d'exploitation ambiante risque de dépasser 40°C (104°F).
PRECAUCIÓN	No instale el instrumento en un entorno en el que la temperatura ambiente de operación pueda exceder los 40°C (104°F).

CAUTION
Make sure the airflow around the front, and back of the device is not restricted.

VORSICHT	Stellen Sie sicher, dass an der Vorderseite, den Seiten und an der Rückseite der Luftstrom nicht behindert wird.
MISE EN GARDE	Vérifiez que rien ne restreint la circulation d'air devant, derrière et sur les côtés du dispositif et qu'elle peut se faire librement.
PRECAUCIÓN	Asegúrese de que el flujo de aire en las inmediaciones de las partes anterior, laterales y posterior del instrumento no esté restringido.

CAUTION
Never leave tools inside the chassis.

VORSICHT	Lassen Sie keine Werkzeuge im Chassis zurück.
MISE EN GARDE	Ne laissez jamais d'outils à l'intérieur du châssis
PRECAUCIÓN	No deje nunca herramientas en el interior del chasis.

CAUTION
Changes or modifications made to this device that are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

VORSICHT	Falls dieses Gerät verändert oder modifiziert wird, ohne die ausdrückliche Genehmigung der für die Einhaltung der Anforderungen verantwortlichen Partei einzuholen, kann dem Benutzer der weitere Betrieb des Gerätes untersagt werden.
MISE EN GARDE	Les éventuelles modifications apportées à cet équipement sans avoir été expressément approuvées par la partie responsable d'en évaluer la conformité sont susceptibles d'annuler le droit de l'utilisateur à utiliser cet équipement.
PRECAUCIÓN	Si se realizan cambios o modificaciones en este dispositivo sin la autorización expresa de la parte responsable del cumplimiento de las normas, la licencia del usuario para operar este equipo puede quedar anulada.

CAUTION
Use the erase startup-config command only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally do erase the configuration on a configured system, enter the write memory command to save the running configuration to the startup-config file.

VORSICHT	Verwenden Sie den Befehl **Erase startup-config** (Löschen Startup-Konfig) nur für neue Systeme. Wenn Sie diesen Befehl in ein bereits konfiguriertes System eingeben, löscht der Befehl die Konfiguration. Falls Sie aus Versehen die Konfiguration eines bereits konfigurierten Systems löschen, geben Sie den Befehl**Write Memory** (Speicher schreiben) ein, um die laufende Konfiguration in der Startup-Konfig-Datei zu speichern.
MISE EN GARDE	N'utilisez la commande **erase startup-config** que pour les nouveaux systèmes. Si vous entrez cette commande sur un système que vous avez déjà configuré, elle efface la configuration. Si vous effacez la configuration par accident sur un système configuré, entrez la commande **write memory** pour enregistrer la configuration actuelle dans le fichier startup-config.
PRECAUCIÓN	Use el comando **erase startup-config** (borrar configuración de inicio) para sistemas nuevos solamente. Si usted introduce este comando en un sistema que ya ha configurado, el comando borrará la configuración. Si usted borra accidentalmente la configuración en un sistema ya configurado, introduzca el comando **write memory** (escribir memoria) para guardar la configuración en ejecución en el archivo startup-config.

CAUTION
Be sure not to exceed the minimum recommended bend radius for the cables: 2" for MRJ-21 cables, and 1.5" for Category 5 (RJ-45) and fiber-optic cables.

VORSICHT	Der empfohlene Mindestbiegeradius für die Kabel darf nicht überschritten werden: 2 Zoll (5,08 cm) bei MRJ-21-Kabeln und 1,5 Zoll (3,81 cm) bei Kabeln der Kategorie 5 (RJ-45) und Glasfaserkabeln.
MISE EN GARDE	Respecter le rayon de courbure minimal recommandé pour les câbles (5,08 cm pour les câbles MRJ-21 et 3,81 cm pour les câbles Ethernet de catégorie 5 (RJ-45) et les fibres optiques).
PRECAUCIÓN	Asegúrese de no exceder el radio de curvatura recomendado para los cables: 2" para los cables MRJ-21 y 1,5" para cables de Categoría 5 (RJ-45) y de fibra óptica.

Electrical cautions

CAUTION
Use a separate branch circuit for each power cord, which provides redundancy in case one of the circuits fails.

VORSICHT	Es empfiehlt sich die Installation eines separaten Stromkreiszweiges für jede Elektroschnur als Redundanz im Fall des Ausfalls eines Stromkreises.
MISE EN GARDE	Utilisez un circuit de dérivation différent pour chaque cordon d'alimentation ainsi, il y aura un circuit redondant en cas de panne d'un des circuits.
PRECAUCIÓN	Use un circuito derivado separado para cada cordón de alimentación, con lo que se proporcionará redundancia en caso de que uno de los circuitos falle.

CAUTION
Ensure that the device does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add the ampere (amp) ratings of all devices installed on the same circuit as the device. Compare this total with the rating limit for the circuit. The maximum ampere ratings are usually printed on the devices near the input power connectors.

VORSICHT	Stromkreise, Verdrahtung und Überlastschutz dürfen nicht durch das Gerät überbelastet werden. Addieren Sie die Nennstromleistung (in Ampere) aller Geräte, die am selben Stromkreis wie das Gerät installiert sind. Somit können Sie feststellen, ob die Gefahr einer Überbelastung der Versorgungsstromkreise vorliegt. Vergleichen Sie diese Summe mit der Nennstromgrenze des Stromkreises. Die Höchstnennströme (in Ampere) stehen normalerweise auf der Geräterückseite neben den Eingangsstromanschlüssen.
MISE EN GARDE	Assurez-vous que le dispositif ne risque pas de surcharger les circuits d'alimentation, le câblage et la protection de surintensité. Pour déterminer le risque de surcharge des circuits d'alimentation, additionnez l'intensité nominale (ampères) de tous les dispositifs installés sur le même circuit que le dispositif en question. Comparez alors ce total avec la limite de charge du circuit. L'intensité nominale maximum en ampères est généralement imprimée sur chaque dispositif près des connecteurs d'entrée d'alimentation.
PRECAUCIÓN	Verifique que el instrumento no sobrecargue los circuitos de corriente, el cableado y la protección para sobrecargas. Para determinar la posibilidad de sobrecarga en los circuitos de suministros, añada las capacidades nominales de corriente (amp) de todos los instrumentos instalados en el mismo circuito que el instrumento. Compare esta suma con el límite nominal para el circuito. Las capacidades nominales de corriente máximas están generalmente impresas en los instrumentos, cerca de los conectores de corriente de entrada.

CAUTION
Before plugging a cable into any port, be sure to discharge the voltage stored on the cable by touching the electrical contacts to ground surface.

VORSICHT	Bevor Sie ein Kabel in einen Anschluss einstecken, entladen Sie jegliche im Kabel vorhandene elektrische Spannung, indem Sie mit den elektrischen Kontakten eine geerdete Oberfläche berühren.
MISE EN GARDE	Avant de brancher un câble à un port, assurez-vous de décharger la tension du câble en reliant les contacts électriques à la terre.
PRECAUCIÓN	Antes de conectar un cable en cualquier puerto, asegúrese de descargar la tensión acumulada en el cable tocando la superficie de conexión a tierra con los contactos eléctricos.

CAUTION
All devices with DC power supplies are intended for installation in restricted access areas only. A restricted access area is a location where access can be gained only by trained service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

VORSICHT	Alle Geräte mit DC-Netzteil sind nur für die Installation in Bereichen mit beschränktem Zugang gedacht. Ein Bereich mit beschränktem Zugang ist ein Ort, zu dem nur ausgebildetes Wartungspersonal mit Spezialwerkzeug, Schloss und Schlüssel oder anderen Sicherheitsvorrichtungen Zugang hat. Dieser Zugang wird von für den Bereich zuständigen Personen überwacht.
MISE EN GARDE	Tous les équipements dotés de sources d'alimentation C.C. sont destinés à être installés uniquement dans des zones à accès réglementé. Une zone à accès réglementé est une zone dont l'accès n'est possible qu'au personnel de service qualifié utilisant un verrou, une clé ou un outil spécial, ou d'autres moyens de sécurité, et qui est contrôlée par les autorités responsables du site.
PRECAUCIÓN	Todos los dispositivos con fuentes de alimentacion de corriente continua (CC) han sido diseñados únicamente para su instalación en áreas restringidas/ zonas de acceso restringido . Se entiende como área de acceso restringido un lugar al que solo puede acceder personal de servicio mediante el uso de una herramienta especial, llave y cerrojo u otro medio de seguridad similar, y que esté controlado por la autoridad responsable de esa ubicación.

CAUTION
All devices with AC power sources are intended for installation in restricted access areas only. A restricted access area is a location where access can be gained only by trained service personnel through the use of a special tool, lock and key, or other means of security.

VORSICHT	Alle Geräte mit Wechselstromquellen sind nur zur Installation in Sperrbereichen bestimmt. Ein Sperrbereich ist ein Ort, zu dem nur ausgebildetes Wartungspersonal mit einem Spezialwerkzeug, Schloss und Schlüssel oder einer anderen Schutzvorrichtung Zugang hat.
MISE EN GARDE	Tous les équipements dotés de sources d'alimentation C.A. sont destinés à être installés uniquement dans des zones à accès réglementé. Une zone à accès réglementé est une zone dont l'accès n'est possible qu'au personnel de service qualifié utilisant un verrou, une clé ou un outil spécial, ou d'autres moyens de sécurité.
PRECAUCIÓN	Todos los dispositivos con fuentes de alimentación de corriente alterna (AC), están diseñados únicamente para su instalación en zonas de acceso restringido. Se entiende como área de acceso restringido un lugar al que solo puede acceder personal de servicio mediante el uso de una herramienta especial, llave y cerrojo u otro medio de seguridad similar, y que esté controlado por la autoridad responsable de esa ubicación.

CAUTION
Remove the power cord from a power supply before you install it in or remove it from the device. Otherwise, the power supply or the device could be damaged as a result. (The device can be running while a power supply is being installed or removed, but the power supply itself should not be connected to a power source.)

VORSICHT	Nehmen Sie vor dem Anschließen oder Abtrennen des Geräts das Stromkabel vom Netzteil ab. Ansonsten könnten das Netzteil oder das Gerät beschädigt werden. (Das Gerät kann während des Anschließens oder Annehmens des Netzteils laufen. Nur das Netzteil sollte nicht an eine Stromquelle angeschlossen sein.)
MISE EN GARDE	Enlevez le cordon d'alimentation d'un bloc d'alimentation avant de l'installer ou de l'enlever du dispositif. Sinon, le bloc d'alimentation ou le dispositif risque d'être endommagé. (Le dispositive peut être en train de fonctionner lorsque vous installez ou enlevez un bloc d'alimentation, mais le bloc d'alimentation lui-même ne doit pas être connecté à une source d'alimentation.)
PRECAUCIÓN	Retire el cordón de corriente del suministro de corriente antes de instalarlo o retírarlo del instrumento. De no hacerse así, el suministro de corriente o el instrumento podrían resultar dañados. (El instrumento puede estar encendido mientras se instala o retira un suministro de corriente, pero el suministro de corriente en sí no deberá conectado a la corriente).

CAUTION
The power supply is designed exclusively for use with the ExtremeSwitching CES Series and ExtremeRouting CER Series devices. The power supply produces extensive power. Installing the power supply in a device other than an ExtremeSwitching CES Series or ExtremeRouting CER Series will cause damage to your equipment.

VORSICHT	Das Netzteil ist ausschließlich für die Verwendung mit den ExtremeSwitching CES-Serie und ExtremeRouting CER-Serie Geräte. Das Netzteil liefert hohe Strompegel. Installation der Stromversorgung in einem anderen als einem ExtremeSwitching CES-Serie oder ExtremeRouting CER-Serie-Gerät Schäden an den Geräten führen.
MISE EN GARDE	L'alimentation est conçu exclusivement pour une utilisation avec les équipements ExtremeSwitching CES série et ExtremeRouting CER série. L'alimentation produit un pouvoir étendu. Installation de l'alimentation dans un équipement autre qu'un ExtremeSwitching CES ou ExtremeRouting CER Series pourrait causer des dommages à votre équipement.
PRECAUCIÓN	La fuente de alimentación está diseñada exclusivamente para el uso con los dispositivos de ExtremeSwitching CES Series y ExtremeRouting CER Series. La fuente de alimentación produce un amplio poder. Instalación de la fuente de alimentación en un dispositivo distinto de la ExtremeSwitching CES Series o ExtremeRouting CER Series causará daños en el equipo.

CAUTION
For the DC input circuit, (DC power supply part number RPS9-DC), make sure there is a 20-amp circuit breaker, minimum -48VDC, double pole, on the input to the terminal block. The input wiring for connection to the product should be copper wire, 12 AWG, marked VW-1, and rated 90 degrees Celsius.

VORSICHT	Für den Eingangs-Gleichstromkreis (Gleichstromnetzteile mit der Teilenr. RPS9-DC) muss gewährleistet warden, dass ein 20 A-Leistungsschalter (min. -48VDC) am Eingang zur Reihenklemme installiert wird. Beim Eingangsdraht für den Anschluss

	am Produkt muss es sich um einen zulässigen Kupferdraht (12 AWG gekennzeichnet mit VW-1), der für mindestens 90° C ausgelegt ist, handeln.
MISE EN GARDE	Pour le circuit d'alimentation C.C.(références du bloc d'alimentation C.C. RPS9-DC), assurez-vous de la présence d'un 20 ampères, minimum -48 V C.C., double coupure, sur l'entrée vers le bloc d'alimentation. Les câbles d'alimentation pour le produit doivent être en fils de cuivre, 3.31 mm² (American Wire Gauge), marqués VW-1 et classés 90 degrés Celsius.
PRECAUCIÓN	Para el circuito de entrada de CC (suministro de corriente continua con No. de referencia RPS9-DC), verifique que haya un cortacircuitos para 20 amperios, mínimo de -48 VCC, bipolar, en la entrada al bloque terminal. El cableado de entrada para la conexión al producto deberá ser catalogado de cobre, 12 AWG, marcado VW-1, y nominal para 90 grados Celsius.

CAUTION

For the DC input circuit to the system of ExtremeRouting MLX-4, ExtremeRouting MLX-8, and ExtremeRouting MLX-16 routers (1800W supply), make sure there is a 60 amp circuit breaker, minimum -48VDC, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be copper wire, 6 AWG, marked VW-1, and rated minimum 90° C.

VORSICHT	Stellen Sie bei der Gleichstromversorgung des Systems bei den Routern ExtremeRouting MLX-4, ExtremeRouting MLX-8 und ExtremeRouting MLX-16 (1800-W-Netzteil) sicher, dass die Anschlussösen des Netzteils mit einem zweipoligen 60-A-Schutzschalter für mindestens -48 V Gleichstrom versehen sind. Die an das Gerät anzuschließenden Eingangsleitungen müssen aus Kupferkabel der Stärke 6 AWG (Bezeichnung VW-1) bestehen und auf eine Temperatur von mindestens 90 °C ausgelegt sein.
MISE EN GARDE	Pour le circuit d'alimentation C.C. du système des routeurs ExtremeRouting MLX-4, ExtremeRouting MLX-8 et ExtremeRouting MLX-16 (alimentation de 1800 W), assurez-vous de la présence d'un disjoncteur bipolaire de 60 ampères, minimum -48 Vcc, sur les cosses d'entrée vers le bloc d'alimentation. Les câbles d'alimentation doivent être en fils de cuivre, 8.37 mm², marqués VW-1 et classés 90°C.
PRECAUCIÓN	Para el circuito de entrada de CC al sistema de los routers ExtremeRouting MLX-4, ExtremeRouting MLX-8, y ExtremeRouting MLX-16 (suministro de 1800 W), asegúrese de que existe un disyuntor bipolar de 60 amperios, de -48 V CC como mínimo, en las terminales de entrada de la fuente de alimentación. El cableado de entrada para la conexión al producto deberá ser de cable de cobre homologado de calibre AWG 6 con clasificación VW-1 para una temperatura mínima de 90 °C.

CAUTION

For the DC input circuit to the system of ExtremeRouting MLX-4, ExtremeRouting MLX-8, and ExtremeRouting MLX-16 routers (1200W supply), make sure there is a 40 amp circuit breaker, minimum -48VDC, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be copper wire, 6 AWG, marked VW-1, and rated minimum 90° C.

VORSICHT	Stellen Sie bei der Gleichstromversorgung des Systems bei den Routern ExtremeRouting MLX-4, ExtremeRouting MLX-8 und ExtremeRouting MLX-16 (1200-W-Netzteil) sicher, dass die Anschlussösen des Netzteils mit einem zweipoligen 40-A-Schutzschalter für mindestens -48 V Gleichstrom versehen sind. Die an das Gerät anzuschließenden Eingangsleitungen müssen aus Kupferkabel der Stärke 6 AWG (Bezeichnung VW-1) bestehen und auf eine Temperatur von mindestens 90 °C ausgelegt sein.
MISE EN GARDE	Pour le circuit d'alimentation C.C. du système des routeurs ExtremeRouting MLX-4, ExtremeRouting MLX-8 et ExtremeRouting MLX-16 (alimentation de 1200 W), assurez-vous de la présence d'un disjoncteur bipolaire de 40 ampères, minimum -48 Vcc, sur les cosses d'entrée vers le bloc d'alimentation. Les câbles d'alimentation doivent être en fils de cuivre, 8.37 mm², marqués VW-1 et classés 90°C.
PRECAUCIÓN	Para el circuito de entrada de CC al sistema de los routers ExtremeRouting MLX-4, ExtremeRouting MLX-8, y ExtremeRouting MLX-16 (suministro de 1200 W), asegúrese de que existe un disyuntor bipolar de 40 amperios, de -48 V CC como mínimo, en las terminales de entrada de la fuente de alimentación. El cableado de entrada para la conexión al producto deberá ser de cable de cobre homologado de calibre AWG 6 con clasificación VW-1 para una temperatura mínima de 90 °C.

CAUTION

For the DC input circuit to the system of an ExtremeRouting MLX-32 (3000W supply) make sure there is a 80 amp circuit breaker, minimum -48Vdc, double pole, on the input lugs to the power supply. The input wiring for connection to the product should be Listed copper wire, 2 AWG, marked VW-1, and rated minimum 90° C.

VORSICHT	Bei der Gleichstromeingangsschaltung zum System eines ExtremeRouting MLX-32 (3000W supply), muss sichergestellt werden, dass an den Eingangskabelschuhen zur Stromversorgung ein zweipoliger Schalter mit UL-Zulassung, 80 Ampere und mindestens -48 V Gleichstrom vorhanden ist. Die Eingangsleitung zum Anschluss an das Produkt sollte als Kupferdraht, angegeben, als VW-1 gekennzeichnet und für mindestens 90 °C bemessen sein.
MISE EN GARDE	Pour le circuit d'alimentation en courant continu du système ExtremeRouting MLX-32 (3000W supply), vérifier la présence d'un disjoncteur bipolaire homologué de 80 A, minimum -48 Vcc, sur l'entrée de l'alimentation. Les câbles d'alimentation du produit doivent être des fils de cuivre homologués de section 33.6 mm², marqués VW-1 et testés à 90° C.
PRECAUCIÓN	Para el circuito de entrada de CC al sistema de un ExtremeRouting MLX-32 (3000W supply), verifique que existe un disyuntor catalogado por UL de 80 amperios, -48VCC como mínimo, bipolar, en las orejetas de entrada a la fuente de alimentación. El cableado de entrada para la conexión al producto deberá ser de cable de cobre catalogado, 2 AWG, marcado con VW-1, y tener una capacidad nominal mínima para 90°C.

CAUTION

For a DC system, use a grounding wire of at least 6 American Wire Gauge (AWG). The 6 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. For the Ground lug, use UL listed Panduit crimp connector, P/N LCD6-10A, and two 10-32, PPH, screws to secure crimp connector to chassis. Grounding position is located on the side of the chassis adjacent ground symbol.

VORSICHT	Für ein Gleichstromsystem ist ein Erdungsdraht (wenigstens 6 AWG) erforderlich. Ein 6 AWGDraht muss mit dem richtigen Werkzeug an einen zugelassenen Crimpverbinder angebracht werden. Der Crimpverbinder dient der Sicherung beider Erdungsschrauben am Gehäuse. Benutzen Sie einen Panduit-Crimpverbinder, Teile Nr. LCD6-10A, als Erdungskabelschuh und zwei 10-32 PPH-Schrauben zum Anbringen des Crimpverbinder am das Gehäuse. Die Erdungsposition befindet sich auf der Gehäuseseite neben dem Erdungssymbol.
MISE EN GARDE	Pour les systèmes C.C., utilisez un fil de mise à la terre d'au moins 6 AWG (American Wire Gauge). Ce fil de 6 AWG doit être relié à un connecteur à sertissage homologué, serti avec l'outil approprié. Le connecteur à sertissage doit permettre la sécurisation aux deux vis de borne de terre sur le boîtier. Pour la patte de mise à la terre, utilisez un connecteur à sertissage UL Panduit, P/N LCD6-10A, et deux vis 10-32, PPH pour attacher le connecteur à sertissage au châssis. La position de mise à la terre se trouve sur le côté du châssis, près du symbole de mise à la terre.
PRECAUCIÓN	Para un sistema de CC, utilice un cable de conexión a tierra de calibre de cable norteamericano (AWG) número 6. El cable 6 AWG deberá acoplarse a un conector engarzado aprobado y engarzado con la herramienta apropiada. El conector engarzado deberá permitir el aseguramiento de ambos tornillos de conexión a tierra en el recinto. Para la lengüeta de masa, emplee un conector engarzado Panduit catalogado por UL, No de pieza LCD6-10A, y dos tornillos PPH, 10-32, para fijar el conector engarzado al chasis. La posición de la conexión a tierra está ubicada en el lado del chasis adyacente al símbolo de conexión a tierra.

CAUTION

For an Extreme Networks AC system, use a ground wire of at least 6 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

VORSICHT	Für ein Extreme Networks Wechselstromsystem ist ein Erdleiter von mindestens 6 AWG (amerikanische Norm für Drahtquerschnitte) zu verwenden. An einem Ende des Erdleiters sollte ein geprüfter gecrimpter Anschluss (mit Chassis bereitgestellt) angebracht sein. Das andere Ende sollte an der Gebäudeerdung angeschlossen werden. Der Anschluss muss mit dem richtigen Werkzeug gecrimpt werden, so dass er an beiden Erdungsschrauben am Gehäuse angeschlossen werden kann.
MISE EN GARDE	Pour un système à alimentation secteur Extreme Networks, utiliser un câble de mise à la terre de calibre AWG 6 (13 mm²) minimum. Ce fil de terre doit être équipé d'un côté d'un connecteur à sertir agréé (fourni avec le châssis), et l'autre extrémité doit être reliée à la terre du bâtiment. Ce connecteur doit être serti à l'aide de l'outil approprié afin d'être raccordé aux deux vis de mise à la terre du boîtier.

PRECAUCIÓN	Para un sistema de CA Extreme Networks, utilice un conductor de tierra de al menos 6 CAE (Calibre de Alambre Estadounidense, American Wire Gauge o AWG en sus siglas en inglés). El conductor de tierra debe tener un conector rizado homologado (suministrado con el chasis) acoplado a un extremo, y el otro extremo debe estar conectado a la tierra del edificio. El conector debe rizarse con la herramienta apropiada, de manera que se conecte a los dos tornillos de tierra del recinto.

CAUTION

For an ExtremeRouting MLX-32 DC system, use a grounding wire of at least 2 American Wire Gauge (AWG). The 2 AWG wire should be attached to an agency-approved crimp connector crimped with the proper tool. The crimp connector should allow for securement to both ground screws on the enclosure. Grounding position is located on the side of the chassis adjacent ground symbol.

VORSICHT	Für ein Gleichstromsystem eines ExtremeRouting MLX-32 ist ein Erdungsdraht (wenigstens 2 AWG) erforderlich. Ein 2 AWGDraht muss mit dem richtigen Werkzeug an einen zugelassenen Crimpverbinder angebracht werden. Der Crimpverbinder dient der Sicherung beider Erdungsschrauben am Gehäuse. Die Erdungsposition befindet sich auf der Gehäuseseite neben dem Erdungssymbol.
MISE EN GARDE	Pour les ExtremeRouting MLX-32 systèmes C.C., utilisez un fil de mise à la terre d'au moins 2 AWG (American Wire Gauge). Ce fil de 2 AWG doit être relié à un connecteur à sertissage homologué, serti avec l'outil approprié. Le connecteur à sertissage doit permettre la sécurisation aux deux vis de borne de terre sur le boîtier. La position de mise à la terre se trouve sur le côté du châssis, près du symbole de mise à la terre.
PRECAUCIÓN	Para un ExtremeRouting MLX-32 sistema de CC, utilice un cable de conexión a tierra de calibre de cable norteamericano (AWG) número 2. El cable 2 AWG deberá acoplarse a un conector engarzado aprobado y engarzado con la herramienta apropiada. El conector engarzado deberá permitir el aseguramiento de ambos tornillos de conexión a tierra en el recinto. La posición de la conexión a tierra está ubicada en el lado del chasis adyacente al símbolo de conexión a tierra.

CAUTION

For an ExtremeRouting MLX-32 AC system, use a ground wire of at least 2 American Wire Gauge (AWG). The ground wire should have an agency-approved crimped connector (provided with the chassis) attached to one end, with the other end attached to building ground. The connector must be crimped with the proper tool, allowing it to be connected to both ground screws on the enclosure.

VORSICHT	Für ein Wechselstromsystem ExtremeRouting MLX-32 ist ein Erdleiter von mindestens 2 AWG (amerikanische Norm für Drahtquerschnitte) zu verwenden. An einem Ende des Erdleiters sollte ein geprüfter gecrimpter Anschluss (mit Chassis bereitgestellt) angebracht sein. Das andere Ende sollte an der Gebäudeerdung angeschlossen werden. Der Anschluss muss mit dem richtigen Werkzeug gecrimpt werden, so dass er an beiden Erdungsschrauben am Gehäuse angeschlossen werden kann.
MISE EN GARDE	Pour le ExtremeRouting MLX-32 avec un système d'alimentation CA, utilisez un câble de mise à la terre de calibre AWG 2. Ce fil de terre doit être équipé d'un côté d'un connecteur à sertir agréé (fourni avec le châssis), et l'autre extrémité doit être reliée à la mise à terre du bâtiment. Ce connecteur doit être serti à l'aide de l'outil approprié afin d'être raccordé aux deux vis de mise à la terre du boîtier.
PRECAUCIÓN	Para un sistema de CA ExtremeRouting MLX-32, utilice un conductor de tierra de al menos 2 CAE (Calibre de Alambre Estadounidense, American Wire Gauge o AWG en sus siglas en inglés). El conductor de tierra debe tener un conector rizado homologado (suministrado con el chasis) acoplado a un extremo, y el otro extremo debe estar conectado a la tierra del edificio. El conector debe rizarse con la herramienta apropiada, de manera que se conecte a los dos tornillos de tierra del recinto.

CAUTION

If you do not install a module or a power supply in a slot, you must keep the slot filler panel in place. If you run the chassis with an uncovered slot, the system will overheat.

VORSICHT	Falls kein Modul oder Netzteil im Steckplatz installiert wird, muss die Steckplatztafel angebracht werden. Wenn ein Steckplatz nicht abgedeckt wird, läuft das System heiß.
MISE EN GARDE	Si vous n'installez pas de module ou de bloc d'alimentation dans un slot, vous devez laisser le panneau du slot en place. Si vous faites fonctionner le châssis avec un slot découvert, le système surchauffera.
PRECAUCIÓN	Si no instala un módulo o un fuente de alimentación en la ranura, deberá mantener el panel de ranuras en su lugar. Si pone en funcionamiento el chasis con una ranura descubierta, el sistema sufrirá sobrecalentamiento.

CAUTION
Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

VORSICHT	Beachten Sie mechanischen Führungen an jeder Seite des Netzteils, das ordnungegemäß in die Führungen gesteckt werden muss. Das Netzteil darf niemals umgedreht eingesteckt werden.
MISE EN GARDE	Suivez attentivement les repères mécaniques de chaque côté du slot du bloc d'alimentation et assurez-vous que le bloc d'alimentation est bien inséré dans les repères. N'insérez jamais le bloc d'alimentation à l'envers.
PRECAUCIÓN	Siga cuidadosamente las guías mecánicas de cada lado de la ranura del suministro de energía y verifique que el suministro de energía está insertado correctamente en las guías. No inserte nunca el suministro de energía de manera invertida.

CAUTION
Removal of ExtremeRouting MLX-32 rear fan modules allows access to bus bars and backplane. Avoid contact with these parts. There are hazardous energy levels at these locations.

VORSICHT	Durch die Entfernung der rückwärtigen ExtremeRouting MLX-32 Ventilatormodule wird der Zugang zu den Sammelschienen und der Rückwandplatine ermöglicht. Kontakt mit diesen Teilen vermeiden. An diesen Stellen liegen gefährliche Stromstärken an.
MISE EN GARDE	La retrait des modules de ventilation de côté arrière du ExtremeRouting MLX-32 permet d'accéder à la distribution électrique et au fond de panier. Éviter tout contact avec ces éléments, car les tensions électriques dans cette zone sont très élevées.
PRECAUCIÓN	El desmontaje de los módulos del ventilador trasero del sistema ExtremeRouting MLX-32 permite el acceso a las barras del bus y a la placa posterior. Evite el contacto con estas piezas. Hay niveles peligrosos de energía en tales lugares.

Cautions related to equipment weight

CAUTION
To prevent damage to the chassis and components, never attempt to lift the chassis using the fan or power supply handles. These handles were not designed to support the weight of the chassis.

VORSICHT	Alle Geräte mit Wechselstromquellen sind nur zur Installation in Sperrbereichen bestimmt. Ein Sperrbereich ist ein Ort, zu dem nur Wartungspersonal mit einem Spezialwerkzeug, Schloss und Schlüssel oder einer anderen Schutzvorrichtung Zugang hat.
MISE EN GARDE	Pour éviter d'endommager le châssis et les composants, ne jamais tenter de soulever le châssis par les poignées du ventilateur ou de l'alimentation. Ces poignées n'ont pas été conçues pour supporter le poids du châssis.
PRECAUCIÓN	Para prevenir daños al chasis y a los componentes, nunca intente levantar el chasis usando las asas de la fuente de alimentación o del ventilador. Tales asas no han sido diseñadas para soportar el peso del chasis.

CAUTION
Do not use the port cover tabs to lift the module. They are not designed to support the weight of the module, which can fall and be damaged.

VORSICHT	Verwenden Sie nicht die Laschen der Anschlussabdeckungen um ein Modul anzuheben. Diese sind nicht auf das Gewicht des Moduls ausgelegt, welches herunterfallen und dabei beschädigt werden kann.
MISE EN GARDE	N'utilisez pas les languettes du boîtier du port pour soulever le module. Elles ne sont pas conçues pour supporter le poids du module, qui peut tomber et être endommagé.
PRECAUCIÓN	No utilice las pestañas de la tapa del puerto para levantar el módulo. No están diseñadas para soportar el peso del módulo, por lo que este podría caerse y resultar dañado.

Danger Notices

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Ein Gefahrenhinweis warnt vor Bedingungen oder Situationen die tödlich sein können oder Sie extrem gefährden können. Sicherheitsetiketten sind direkt auf den jeweiligen Produkten angebracht um vor diesen Bedingungen und Situationen zu warnen.

Un énoncé de danger indique des conditions ou des situations potentiellement mortelles ou extrêmement dangereuses. Des étiquettes de sécurité sont posées directement sur le produit et vous avertissent de ces conditions ou situations.

Una advertencia de peligro indica condiciones o situaciones que pueden resultar potencialmente letales o extremadamente peligrosas. También habrá etiquetas de seguridad pegadas directamente sobre los productos para advertir de estas condiciones o situaciones.

General dangers

DANGER
The procedures in this manual are for qualified service personnel.

GEFAHR	Die Vorgehensweisen in diesem Handbuch sind für qualifiziertes Servicepersonal bestimmt.
DANGER	Les procédures décrites dans ce manuel doivent être effectuées par un personnel de maintenance qualifié.
PELIGRO	Los procedimientos de este manual deben llevarlos a cabo técnicos cualificados.

DANGER
Be careful not to accidently insert your fingers into the fan tray while removing it from the chassis. The fan may still be spinning at a high speed.

GEFAHR	Die Finger dürfen nicht versehentlich in das Ventilatorblech gesteckt werden, wenn dieses vom Gehäuse abgenommen wird. Der Ventilator kann sich unter Umständen noch mit hoher Geschwindigkeit drehen.
DANGER	Faites attention de ne pas insérer vos doigts accidentellement dans le boîtier du ventilateur lorsque vous le retirez du châssis. Il est possible que le ventilateur tourne encore à grande vitesse.
PELIGRO	Procure no insertar los dedos accidentalmente en la bandeja del ventilador cuando esté desmontando el chasis. El ventilador podría estar girando a gran velocidad.

Electrical dangers

DANGER
Before beginning the installation, see the precautions in "Power precautions."

GEFAHR	Vor der Installation siehe Vorsichtsmaßnahmen unter "Power Precautions" (Vorsichtsmaßnahmen in Bezug auf elektrische Ablagen).
DANGER	Avant de commencer l'installation, consultez les précautions décrites dans "Power Precautions" (Précautions quant à l'alimentation).
PELIGRO	Antes de comenzar la instalación, consulte las precauciones en la sección "Power Precautions" (Precauciones sobre corriente).

DANGER
Disconnect the power cord from all power sources to completely remove power from the device.

GEFAHR	Ziehen Sie das Stromkabel aus allen Stromquellen, um sicherzustellen, dass dem Gerät kein Strom zugeführt wird.

DANGER	Débranchez le cordon d'alimentation de toutes les sources d'alimentation pour couper complètement l'alimentation du dispositif.
PELIGRO	Para desconectar completamente la corriente del instrumento, desconecte el cordón de corriente de todas las fuentes de corriente.

DANGER
If the installation requires a different power cord than the one supplied with the device, make sure you use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

GEFAHR	Falls für die Installation ein anderes Stromkabel erforderlich ist (wenn das mit dem Gerät gelieferte Kabel nicht passt), müssen Sie sicherstellen, dass Sie ein Stromkabel mit dem Siegel einer Sicherheitsbehörde verwenden, die für die Zertifizierung von Stromkabeln in Ihrem Land zuständig ist. Das Siegel ist Ihre Garantie, dass das Stromkabel sicher mit Ihrem Gerät verwendet werden kann.
DANGER	Si l'installation nécessite un cordon d'alimentation autre que celui fourni avec le dispositif, assurez-vous d'utiliser un cordon d'alimentation portant la marque de l'organisation responsable de la sécurité qui définit les normes et régulations pour les cordons d'alimentation dans votre pays. Cette marque vous assure que vous pouvez utiliser le cordon d'alimentation avec le dispositif en toute sécurité.
PELIGRO	Si la instalación requiere un cordón de corriente distinto al que se ha suministrado con el instrumento, verifique que usa un cordón de corriente que venga con la marca de la agencia de seguridad que defina las regulaciones para cordones de corriente en su país. Esta marca será su garantía de que el cordón de corriente puede ser utilizado con seguridad con el instrumento.

DANGER
For safety reasons, the ESD wrist strap should contain a series 1 megaohm resistor.

GEFAHR	Aus Sicherheitsgründen sollte ein EGB-Armband zum Schutz von elektronischen gefährdeten Bauelementen mit einem 1 Megaohm-Reihenwiderstand ausgestattet sein.
DANGER	Pour des raisons de sécurité, la dragonne ESD doit contenir une résistance de série 1 méga ohm.
PELIGRO	Por razones de seguridad, la correa de muñeca ESD deberá contener un resistor en serie de 1 mega ohmio.

DANGER
Batteries used for RTC/NVRAM backup are not located in operator-access areas. There is a risk of explosion if a battery is replace by an incorrect type. Dispose of used components with batteries according to local ordinance and regulations.

GEFAHR	Die für die RTC/NVRAM-Sicherung verwendeten Batterien, befinden sich nicht in für den Bediener zugänglichen Bereichen. Bei Ersetzen der Batterie durch einen falschen Typ besteht Explosionsgefahr. Entsorgen Sie gebrauchte Komponenten mit Batterien gemäß den lokalen Auflagen und Vorschriften.
DANGER	Les batteries utilisées pour la sauvegarde RTC/NVRAM ne se trouvent pas dans des zones accessibles par l'opérateur. Il y a un risque d'explosion si une batterie est remplacée par un type de batterie incompatible. Éliminez les composants utilisés avec des batteries conformément aux ordonnances et aux règlements locaux.
PELIGRO	Las baterías usadas para respaldo de RTC/NVRAM no se encuentran en areas de acceso del operador. Existe riesgo de explosión si una batería es remplazada por un tipo incorrecto. Deshágase de los componentes usados con las baterías según las politicas y regulaciones locales.

DANGER
Make sure that the power source circuits are properly grounded, then use the power cord supplied with the device to connect it to the power source.

GEFAHR	Stellen Sie sicher, dass die Stromkreise ordnungsgemäß geerdet sind. Benutzen Sie dann das mit dem Gerät gelieferte Stromkabel, um es an die Srromquelle anzuschließen.
DANGER	Vérifiez que les circuits de sources d'alimentation sont bien mis à la terre, puis utilisez lecordon d'alimentation fourni avec le dispositif pour le connecter à la source d'alimentation.

PELIGRO	Verifique que circuitos de la fuente de corriente están conectados a tierra correctamente; luego use el cordón de potencia suministrado con el instrumento para conectarlo a la fuente de corriente

DANGER

Make sure to choose the appropriate circuit device depending on the number of AC power supplies installed in the chassis. The minimum current draw for the system is one AC power supply.

GEFAHR	Je nach Anzahl der Wechselstrom-Netzteile im Gehäuse muss das passende Stromgerät ausgewählt werden. Für die Mindeststromentnahme für das System ist ein Wechselstrom-Netzteil erforderlich.
DANGER	Assurez-vous de choisir le dispositif de circuit approprié selon le nombre de blocs d'alimentation C.A. installés dans le châssis. L'appel de courant minimum pour le système est d'un bloc d'alimentation C.A.
PELIGRO	Verifique que elige el instrumento para circuitos apropiado dependiendo del número de suministros de energía de CC instalados en el chasis. La llamada de corriente mínima para el sistema es de un suministro de energía de CC.

DANGER

The intra-building port or ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port or ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 5) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

GEFAHR	Die gebäudeinternen Anschlüsse des Geräts bzw. der Unterbaugruppe sind nur zur Verbindung mit gebäudeinternen bzw. nicht freiliegenden Drähten und Kabeln geeignet. Die gebäudeinternen Anschlüsse des Geräts bzw. der Baugruppe DÜRFEN NICHT metallisch mit Schnittstellen verbunden werden, die an Außenbereiche (OSP) oder deren Verdrahtung angeschlossen sind. Diese Schnittstellen sind ausschließlich zur Verwendung als gebäudeinterne Schnittstellen ausgelegt (Anschlüsse des Typs 2 oder 4 gemäß GR-1089-CORE, Ausgabe 5) und müssen von den freiliegenden OSP-Kabeln isoliert werden. Eine hinzugefügte Primärschutzeinrichtung ist kein ausreichender Schutz gegen den metallischen Anschluss dieser Schnittstellen an die OSP-Verdrahtung.
DANGER	Le ou les ports des connexions intra-bâtiment ou un sous-ensemble sont uniquement acceptable à une connexion intra-bâtiment ou une connexion avec du câblage non exposé. Il est rigoureusement interdit d'établir un contact métallique entre le ou les ports intra-bâtiment ou sous-ensemble, et des interfaces connectées à des installations extérieures (OSP) ou à leur câblage. Ces interfaces sont spécifiquement conçues pour un usage intra-bâtiment (les ports de Type 2 ou Type 4 comme décrits dans le document GR-1089-CORE, volume 5) et elles doivent être isolées de tout câblage exposé dans les installations extérieures (OSP). L'ajout des équipements de protection primaire (Primary Protectors) n'offre pas une protection suffisante pour permettre un raccordement par contact métallique au câblage extérieur (OSP).
PELIGRO	Los puertos del equipo o del sistema secundario situados en el interior de un edificio únicamente podrán conectarse a instalaciones eléctricas o cableados que se encuentren dentro del edificio o que no estén expuestos. Los puertos del equipo o del sistema secundario situados en el interior del edificio NO DEBEN conectarse metálicamente a interfaces que se encuentren conectadas a la planta exterior (OSP por sus siglas en inglés) o a su sistema eléctrico. Dichas interfaces han sido diseñadas para uso exclusivo en el interior de un edificio (puertos Tipo 2 o Tipo 4, según lo descrito en GR-1089-CORE, Número 5) y deben aislarse del cableado de la OSP expuesto. La incorporación de Protectores Primarios no proporciona protección suficiente para conectar dichas interfaces metálicamente al sistema eléctrico de la OSP.

DANGER

High Touch Current. Earth connection essential before connecting supply.

GEFAHR	Hoher Ableitstrom. Vor Anschluss ans Netz Schutzerdung herstellen.
DANGER	Courant de fuite élevé. Mise à la terre obligatoire avant la connexion de l'alimentation.
PELIGRO	Alta tensión al tacto. La conexión a tierra es esencial antes de conectar la alimentación.

Dangers related to equipment weight

DANGER
Make sure the rack housing the device is adequately secured to prevent it from becoming unstable or falling over.

GEFAHR	Stellen Sie sicher, dass das Gestell für die Unterbringung des Geräts auf angemessene Weise gesichert ist, so dass das Gestell oder der Schrank nicht wackeln oder umfallen kann.
DANGER	Vérifiez que le bâti abritant le dispositif est bien fixé afin qu'il ne devienne pas instable ou qu'il ne risque pas de tomber.
PELIGRO	Verifique que el bastidor que alberga el instrumento está asegurado correctamente para evitar que pueda hacerse inestable o que caiga.

DANGER
Mount the devices you install in a rack as low as possible. Place the heaviest device at the bottom and progressively place lighter devices above.

GEFAHR	Montieren Sie die Geräte im Gestell so tief wie möglich. Platzieren Sie das schwerste Gerät ganz unten, während leichtere Geräte je nach Gewicht (je schwerer desto tiefer) darüber untergebracht werden.
DANGER	Montez les dispositifs que vous installez dans un bâti aussi bas que possible. Placez le dispositif le plus lourd en bas et le plus léger en haut, en plaçant tous les dispositifs progressivement de bas en haut du plus lourd au plus léger.
PELIGRO	Monte los instrumentos que instale en un bastidor lo más bajos posible. Ponga el instrumento más pesado en la parte inferior y los instrumentos progresivamente más livianos más arriba.

DANGER
A fully populated chassis is heavy. TWO OR MORE PEOPLE ARE REQUIRED WHEN LIFTING, HANDLING, OR MOUNTING THESE DEVICES.

GEFAHR	Ein voll bestücktes Gehäuse ist schwer. ZUM ANHEBEN, HANDHABEN ODER MONTIEREN DIESER GERÄTE SIND MINDESTENS ZWEI PERSONEN ERFORDERLICH.
DANGER	Les châssis sont lourds quand ils sont entièrement remplis. POUR SOULEVER, MANIPULER OU MONTER CES DISPOSITIFS, DEUX PERSONNES MINIMUM SONT NÉCESSAIRES.
PELIGRO	Un chasis muy concurrido es muy pesado. SE REQUIEREN DOS O MÁS PERSONAS CUANDO SE VAYA A ALZAR, MANEJAR O MONTAR ESTE DISPOSITIVO.

DANGER
Do not attempt to lift an ExtremeRouting MLX-32 chassis. It is extremely heavy. REMOVE THE POWER SUPPLIES AND INTERFACE MODULES FIRST (management, switch fabric, and all line cards). Use a mechanical lifting device to lift the chassis. Four or more people are required to position the unpopulated chassis into the rack.

GEFAHR	Nicht versuchen, ein ExtremeRouting MLX-32 Chassis anzuheben. Es ist sehr schwer. ZUERST DIE STROMVERSORGUNGEN UND SCHNITTSTELLENMODULE ENTFERNEN (Management, Switch-Fabric und alle Line-Cards). Das Chassis mit Hilfe einer mechanischen Hebevorrichtung anheben. Mindestens vier Personen sind erforderlich, um das unbeladene Chassis im Rack zu positionieren.
DANGER	Ne jamais tenter de soulever un châssis ExtremeRouting MLX-32 car il est alors extrêmement lourd. DÉPOSER AU PRÉALABLE LES ALIMENTATIONS ÉLECTRIQUES ET LES MODULES D'INTERFACE (supervision, matrice de commutation et cartes de lignes). Pour soulever le châssis, utiliser un appareil élévateur. Quatre personnes au moins sont nécessaires pour positionner dans le rack le châssis vidé de ses éléments.
PELIGRO	No trate de levantar un chasis ExtremeRouting MLX-32. Es extremadamente pesado. QUITE PRIMERO LOS MÓDULOS DE INTERFAZ Y DE ALIMENTACIÓN (administración, matriz de conmutación, y todas las tarjetas de línea). Utilice un elevador mecánico para levantar el chasis. Hacen falta cuatro personas o más para colocar el chasis no poblado en el interior del armazón.

DANGER
The ExtremeRouting MLX-32 fan assembly is heavy and will be off-balance as you remove it. Use both hands on the handle.

GEFAHR	Die ExtremeRouting MLX-32-Ventilatoreinheit ist schwer und kommt aus dem Gleichgewicht, wenn sie entfernt wird. Den Griff mit beiden Händen anfassen.
DANGER	Le module de ventilation du ExtremeRouting MLX-32 est lourd et peut déséquilibrer lors de la dépose. Tenir la poignée à l'aide des deux mains.
PELIGRO	La unidad del ventilador del sistema ExtremeRouting MLX-32 es pesada y quedará desequilibrada al desmontarla. Agarre el asa con las dos manos.

Laser dangers

DANGER
All fiber-optic interfaces use Class 1 lasers.

GEFAHR	Alle Glasfaser-Schnittstellen verwenden Laser der Klasse 1.
DANGER	Toutes les interfaces en fibre optique utilisent des lasers de classe 1.
PELIGRO	Todas las interfaces de fibra óptica utilizan láser de clase 1.

DANGER
Laser Radiation. Do Not View Directly with Optical Instruments. Class 1M Laser Products.

GEFAHR	Laserstrahlung! Schauen Sie nicht direkt mit optischen Instrumenten in den Laserstrahl herein. Klasse 1M Laserprodukte.
DANGER	Rayonnement de laser. Ne regardez pas directement avec des instruments optiques. Produits de laser de classe 1M.
PELIGRO	Radiacion de Laser. No vea directamente con Instrumentos Opticos. Clase 1M de Productos de Laser.
警告	レーザ放射 光学器具で直接ビームを見ないこと クラス１ M レーザ製品