BROCADE

Brocade® MLXe® and Brocade NetIron® CER 2000 Series Ethernet Routers

FIPS 140-2 Non-Proprietary Security Policy

Level 2 with Design Assurance Level 3 Validation

Document Version 1.6

June 1, 2014

Revision History

Revision Date	Revision	Summary of Changes
6/5/13	1.0	First submitted version
6/6/13	1.1	Changed references to TLS to TLS (non-compliant) to be in alignment with IG D.8 scenario 4
6/18/13	1.2	Added “Hereafter this non-compliance applies to all references to SSH, TLS and SNMPv3” to paragraph 3 of chapter 6 Services. Removed “(non-compliant)” throughout the document next to SSH, TLS and SNMPv3. Since we are not claiming compliance to SP 800-135, the blanket statement in Chapter 6 should suffice. Added “and TLS” to SSHv2 KDF references.
3/5/14	1.3	Changed RSA/DSA/DH to noncompliant per 800-131a
3/20/14	1.4	Updated note under table 24 to clarify details on RSA and DSA non-compliancy.
4/12/14	1.5	Updated sections 6 and 7 to reflect disallowed services.
6/1/14	1.6	Separated approved from non-approved services section 7.3

This Brocade Communications Systems Security Policy for Brocade MLXe and Brocade NetIron CER 2000 series embodies Brocade Communications Systems' confidential and proprietary intellectual property. Brocade Systems retains all title and ownership in the Specification, including any revisions.

This Specification is supplied AS IS and may be reproduced only in its original entirety [without revision]. Brocade Communications Systems makes no warranty, either express or implied, as to the use, operation, condition, or performance of the specification, and any unintended consequence it may on the user environment.

Table of Contents

Table of Tables

Table of Figures

Introduction

Brocade MLXe Series routers feature industry-leading 100 Gigabit Ethernet (GbE), 10 GbE, and 1 GbE wire-speed density; rich IPv4, IPv6, Multi-VRF, MPLS, and Carrier Ethernet capabilities without compromising performance; and advanced Layer 2 switching. Built upon Brocade's sixth-generation architecture and terabit-scale switch fabrics, the Brocade MLXe Series has a proven heritage with more than 9000 routers deployed worldwide. Internet Service Providers (ISPs), transit networks, Content Delivery Networks (CDNs), hosting providers, and Internet Exchange Points (IXPs) rely on these routers to meet skyrocketing traffic requirements and reduce the cost per bit. By leveraging the Brocade MLXe Series, mission-critical data centers can support more traffic, achieve greater virtualization, and provide cloud services using less infrastructure—thereby simplifying operations and reducing costs. Moreover, the Brocade MLXe Series can reduce complexity in large campus networks by collapsing core and aggregation layers, as well as providing connectivity between sites using MPLS/VPLS.

The Brocade NetIron CER 2000 Series is a family of compact 1U routers that are purpose-built for high-performance Ethernet edge routing and MPLS applications. These fixed-form routers can store a complete Internet table and support advanced MPLS features such as Traffic Engineering and VPLS. They are ideal for supporting a wide range of applications in Metro Ethernet, data center and campus networks. The NetIron CER 2000 is available in 24- and 48-port 1 Gigabit Ethernet (GbE) copper and hybrid fiber configurations with two optional 10 GbE uplink ports. To help ensure high performance, all the ports are capable of forwarding IP and MPLS packets at wire speed without oversubscription. With less than 5 watts/Gbps of power consumption, service providers can push up to 136 Gbps of triple-play services through the NetIron CER 2000 while reducing their carbon footprint.

1 Overview

Brocade routers provide high-performance routing to service providers, metro topologies, and Internet Exchange Points. Each router is a multi-chip standalone cryptographic module. Each device has an opaque enclosure with tamper detection tape for detecting any unauthorized physical access to the device. The NetIron family includes both chassis and fixed-port devices.

Brocade MLXe series devices are chassis devices. Each MLXe chassis contains slots for MR and MR2 management cards, Switch Fabric Modules (SFM), and interface modules. The SFM pass data packets between the various modules. The interface modules themselves forward data without any cryptographic operation or pass data packets to a management module, if any cryptographic operation has to be performed.

The cryptographic boundary of a Brocade MLXe series device is a chassis with two like management cards; one management module runs in active mode while the other is in standby mode. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies are covered by opaque filler panels, which are part of the cryptographic boundary when the secondary redundant power supplies are not used. Unpopulated switch fabric module and interface modules slots are covered by opaque filler panels, which are part of the crypto boundary.

The cryptographic boundary of a CER 2000 series device is the outer perimeter of the metal chassis including the removable cover. Within the NetIron family, the CER 2000 series are fixed-port devices.

For an MLXe or CER device to operate as a validated cryptographic module, the tamper evident seals supplied in Brocade XBR-000195 must be installed as defined in Appendix A.

The security officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The security officer shall maintain a serial number inventory of all used and unused tamper evident seals. The security officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The security officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The security officer is responsible for returning a module to a validated cryptographic state after any intentional or unintentional reconfiguration of the physical security measures.

2 Brocade MLXe series

Note: The modules have been validated with each of the following separate firmware versions:

Table 1 MLXe Series Firmware Version

Firmware
IronWare Release R05.3.00ea
IronWare Release R05.4.00cb

Table 2 MLXe Series Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-4-MR-M-AC	80-1006853-01	Brocade MLXe-4 AC system with 2 high speed switch fabric modules, 1 AC 1200 W power supply, 4 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-4-MR-M-DC	80-1006854-01	Brocade MLXe-4 DC system with 2 high speed switch fabric modules, 1 DC 1200 W power supply, 4 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-8-MR-M-AC	80-1004809-04	Brocade MLXe-8 AC system with 2 high speed switch fabric modules, 2 AC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-8-MR-M-DC	80-1004811-04	Brocade MLXe-8 DC system with 2 high speed switch fabric modules, 2 DC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included
BR-MLXE-16-MR-M-AC	80-1006820-02	Brocade MLXe-16 AC system with 3 high speed switch fabric modules, 4 AC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-16-MR-M-DC	80-1006822-02	Brocade MLXe-16 DC system with 3 high speed switch fabric modules, 4 DC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-4-MR2-M-AC	80-1006870-01	Brocade MLXe-4, AC system with 1 MR2 management module, 2 high speed switch fabric modules, 1 AC 1800 W power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-4-MR2-M-DC	80-1006872-01	Brocade MLXe-4, DC system with 1 MR2 management module, 2 high speed switch fabric modules, 1 1800 W DC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.

SKU	MFG Part Number	Brief Description
BR-MLXE-8-MR2-M-AC	80-1007225-01	Brocade MLXe-8 AC system with 1 MR2 management module, 2 high speed switch fabric modules, 2 1800 W AC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-8-MR2-M-DC	80-1007226-01	Brocade MLXe-8 DC system with 1 MR2 management module, 2 high speed switch fabric modules, 21800 W DC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-16-MR2-M-AC	80-1006827-02	Brocade MLXe-16 AC system with 1 MR2 management module, 3 high speed switch fabric modules, 4 AC1800 W power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-16-MR2-M-DC	80-1006828-02	Brocade MLXe-16 DC system with 1 MR2 management module, 3 high speed switch fabric modules, 4 DC 1800 W power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included

Table 3 MLXe Management Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-MLX-MR	80-1006778-01	NetIron MLX Series management module with 1 GB ECC memory, dual PCMCIA slots, EIA/TIA-232 (RS- 232) serial console port and 10/100/1000 Ethernet port for out-of band management
BR-MLX-MR2-M	80-1005643-01	MLXE/MLX GEN2, Management module for 4, 8 and 16-Slot Systems. Includes 4 GB RAM, 1 internal Compact Flash

Table 4 MLXe Switch Fabric Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-X-4-HSF	80-1003891-02	MLXe/MLX/XMR high speed switch fabric module for 4-slot chassis
NI-X-16-8-HSF	80-1002983-01	MLXe/MLX/XMR high speed switch fabric module for 8-slot and 16-slot chassis

Table 5 MLXe Power Supply Module Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-ACPWR-1800	80-1003971-01	16-slot, 8-slot and 4-slot MLXe AC 1800W power supply
BR-MLXE-DCPWR-1800	80-1003972-01	16-slot, 8-slot and 4-slot MLXe DC 1800W power supply
NI-X-ACPWR	80-1003811-02	16-slot, 8-slot and 4-slot MLXe AC 1200W power supply
NI-X-DCPWR	80-1002756-03	16-slot, 8-slot and 4-slot MLXe DC 1200W power supply

Table 6 MLXe Fan Module Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-4-FAN	80-1004114-01	MLXe-4 exhaust fan assembly kit
BR-MLXE-8-FAN	80-1004113-01	MLXe-8 exhaust fan assembly kit
BR-MLXE-16-FAN	80-1004112-01	MLXe-16 exhaust fan assembly kit

Table 7 MLXe Filler Panel Part Numbers

SKU	MFG Part Number	Brief Description
NI-X-MPNL	80-1004760-02	NetIron XMR/MLX Series management module blank panel
NI-X-IPNL	80-1006511-02	NetIron XMR/MLX Series interface module blank panel
NI-X-SF3PNL	80-1004757-02	NetIron XMR/MLX switch fabric module blank panel for 16- and 8-slot chassis
NI-X-SF1PNL	80-1003009-01	NetIron XMR/MLX switch fabric module blank panel for 4-slot chassis
NI-X-PWRPNL	80-1003052-01	NetIron XMR/MLX power supply blank panel for 16-and 8-slot chassis
NI-X-PWRPNL-A	80-1003053-01	NetIron XMR/MLX power supply blank panel for 4-slot chassis

Table 8 Validated MLXe Configurations

Validated MLXe Configurations	
MLXe Model	SKUs (Count)
MLXe-4	Chassis: BR-MLXE-4-MR-M-AC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-4-HSF (2) Switch fabric Module Filler Panels: NI-X-SF1PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (4) Fan Modules: BR-MLXE-4-FAN (4) AC Power Supply Modules: NI-X-ACPWR (1) Power Supply Filler Panels: NI-X-PWRPNL-A (3)
	Chassis: BR-MLXE-4-MR-M-DC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-4-HSF (2) Switch fabric Module Filler Panels: NI-X-SF1PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (4) Fan Modules: BR-MLXE-4-FAN (4) DC Power Supply Modules: NI-X-DCPWR (1) Power Supply Filler Panels: NI-X-PWRPNL-A (3)

Validated MLXe Configurations	
MLXe Model	SKUs (Count)
MLXe-4	Chassis: BR-MLXE-4-MR2-M-AC Management Module: BR-MLX-MR2-M (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-4-HSF (2) Switch fabric Module Filler Panels: NI-X-SF1PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (4) Fan Modules: BR-MLXE-4-FAN (4) AC Power Supply Modules: BR-MLXE-ACPWR-1800 (1) Power Supply Filler Panels: NI-X-PWRPNL-A (3)
	Chassis: BR-MLXE-4-MR2-M-DC Management Module: BR-MLX-MR2-M (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-4-HSF (2) Switch fabric Module Filler Panels: NI-X-SF1PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (4) Fan Modules: BR-MLXE-4-FAN (4) DC Power Supply Modules: BR-MLXE-DCPWR-1800 (1) Power Supply Filler Panels: NI-X-PWRPNL-A (3)
MLXe-8	Chassis: BR-MLXE-8-MR-M-AC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (2) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (8) Fan Modules: BR-MLXE-8-FAN (2) AC Power Supply Modules: NI-X-ACPWR (2) Power Supply Filler Panels: NI-X-PWRPNL (2)
	Chassis: BR-MLXE-8-MR-M-DC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (2) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (8) Fan Modules: BR-MLXE-8-FAN (2) DC Power Supply Modules: NI-X-DCPWR (2) Power Supply Filler Panels: NI-X-PWRPNL(2)

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**
MLXe-8	Chassis: BR-MLXE-8-MR2-M-AC Management Module: BR-MLX-MR2-M (2) Management Module Filler Panel: None Switch Fabric Modules: NI-X-16-8-HSF (2) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (8) Fan Modules: BR-MLXE-8-FAN (2) AC Power Supply Modules: BR-MLXE-ACPWR-1800 (2) Power Supply Filler Panels: NI-X-PWRPNL (2)
	Chassis: BR-MLXE-8-MR2-M-DC Management Module: : BR-MLX-MR2-M (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (2) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (8) Fan Modules: BR-MLXE-8-FAN (2) DC Power Supply Modules BR-MLXE-DCPWR-1800 (2) Power Supply Filler Panels: NI-X-PWRPNL(2)
MLXe-16	Chassis: BR-MLXE-16-MR-M-AC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (3) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (16) Fan Modules: BR-MLXE-16-FAN (2) AC Power Supply Modules: NI-X-ACPWR (4), Power Supply Filler Panels: NI-X-PWRPNL (4)
	Chassis: BR-MLXE-16-MR-M-DC Management Module: NI-MLX-MR (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (3) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (16) Fan Modules: BR-MLXE-16-FAN (2) DC Power Supply Modules: NI-X-DCPWR (4), Power Supply Filler Panels: NI-X-PWRPNL (4)

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**
MLXe-16	Chassis: BR-MLXE-16-MR2-M-AC Management Module: BR-MLX-MR2-M (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (3) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (16) Fan Modules: BR-MLXE-16-FAN (2) AC Power Supply Modules: BR-MLXE-ACPWR-1800 (4) Power Supply Filler Panels: NI-X-PWRPNL (4)
	Chassis: BR-MLXE-16-MR2-M-DC Management Module: BR-MLX-MR2-M (2) Management Module Filler Panels: None Switch Fabric Modules: NI-X-16-8-HSF (3) Switch fabric Module Filler Panels: NI-X-SF3PNL (1) Interface Modules: None Interface Module Filler Panels: NI-X-IPNL (16) Fan Modules: BR-MLXE-16-FAN (2) DC Power Supply Modules: BR-MLXE-DCPWR-1800 (4) Power Supply Filler Panels: NI-X-PWRPNL (4)

Figure 1 illustrates an MLXe-4 cryptographic module with two MR management modules. Table 8 defines the configuration of the validated MLXe-4 cryptographic module. Indicators are provided in Figure 1 to define the location of the management modules, switch fabric modules and power supply module.

Figure 1 MLXe-4 Cryptographic Module with MR Management Modules

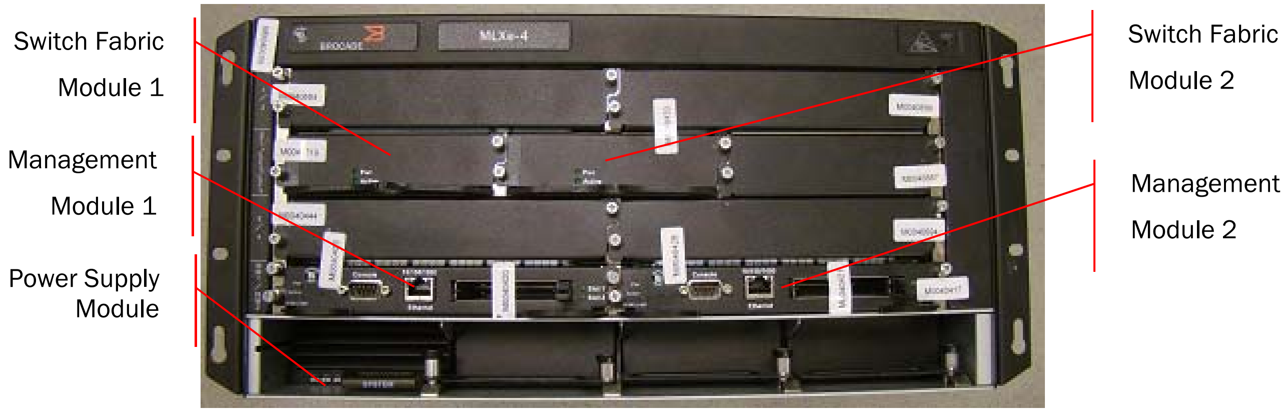


Figure 2 illustrates an MLXe-4 cryptographic module with two MR2 management modules. Table 8 defines the configuration of the validated MLXe-4 cryptographic module. Indicators are provided in Figure 2 to define the location of the management modules, switch fabric modules and power supply module. .

Figure 2 MLXe-4 Cryptographic Module with MR2 Management Modules

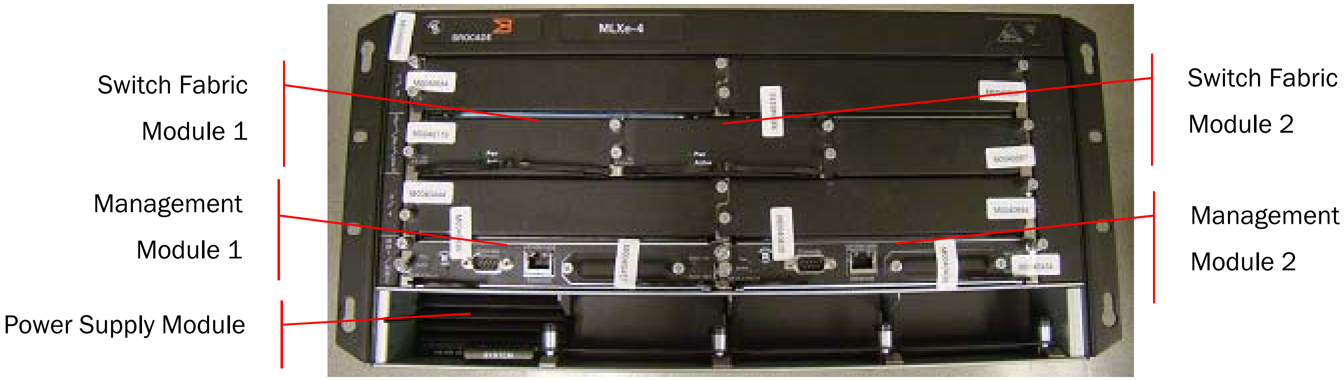


Figure 3 illustrates an MLXe-8 cryptographic module with two MR management modules. Table 8 defines the configuration of the validated MLXe-8 cryptographic module. Indicators are provided in Figure 3 to define the location of the management modules, switch fabric modules and power supply modules.

Figure 3 MLXe-8 Cryptographic Module with MR Management Modules

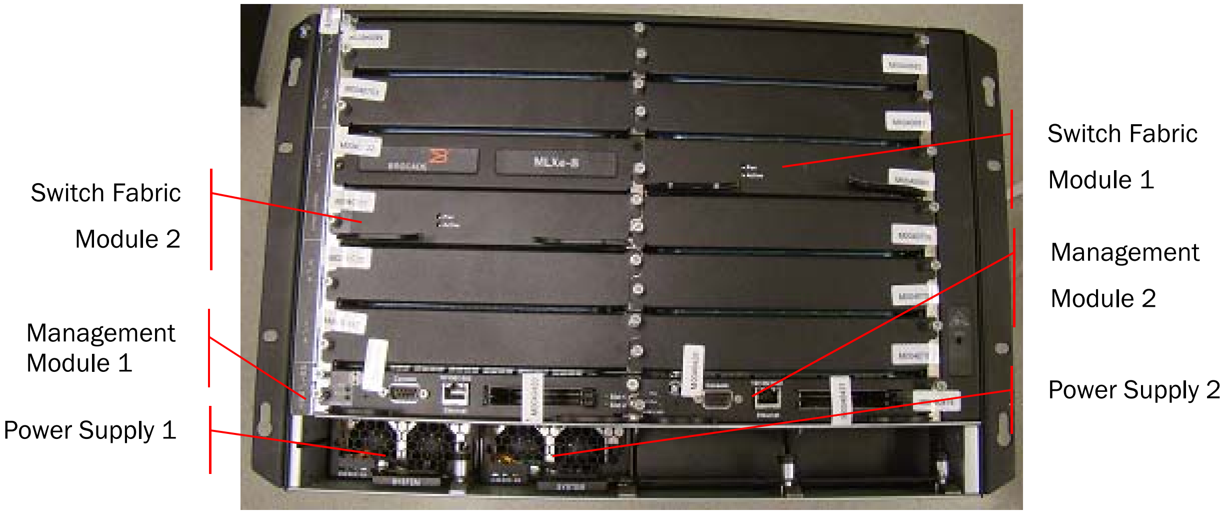


Figure 4 illustrates an MLXe-8 cryptographic module with two MR2 management modules. Table 8 defines the configuration of the validated MLXe-8 cryptographic module. Indicators are provided in Figure 4 to define the location of the management modules, switch fabric modules and power supply modules.

Figure 4 MLXe-8 Cryptographic Module with MR2 Management Modules

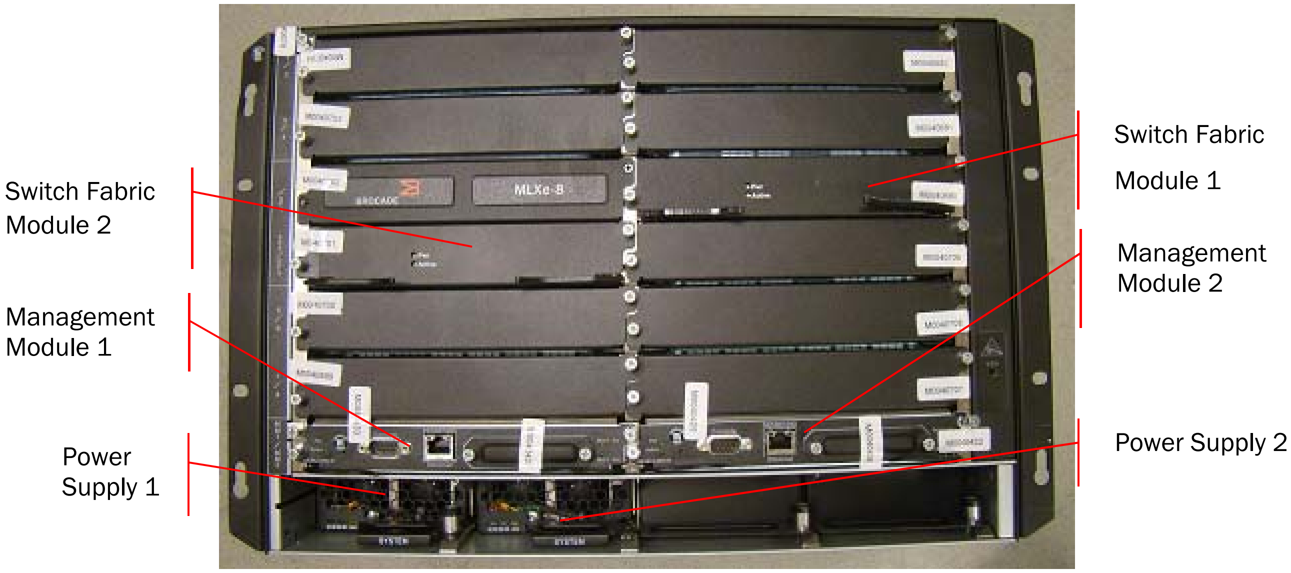


Figure 5 illustrates an MLXe-16 cryptographic module with two MR management modules. Table 8 defines the configuration of the validated MLXe-16 cryptographic module. Indicators are provided in Figure 5 to define the location of the management modules, switch fabric modules and power supply modules.

Figure 5 MLXe-16 Cryptographic Module with MR Management Modules

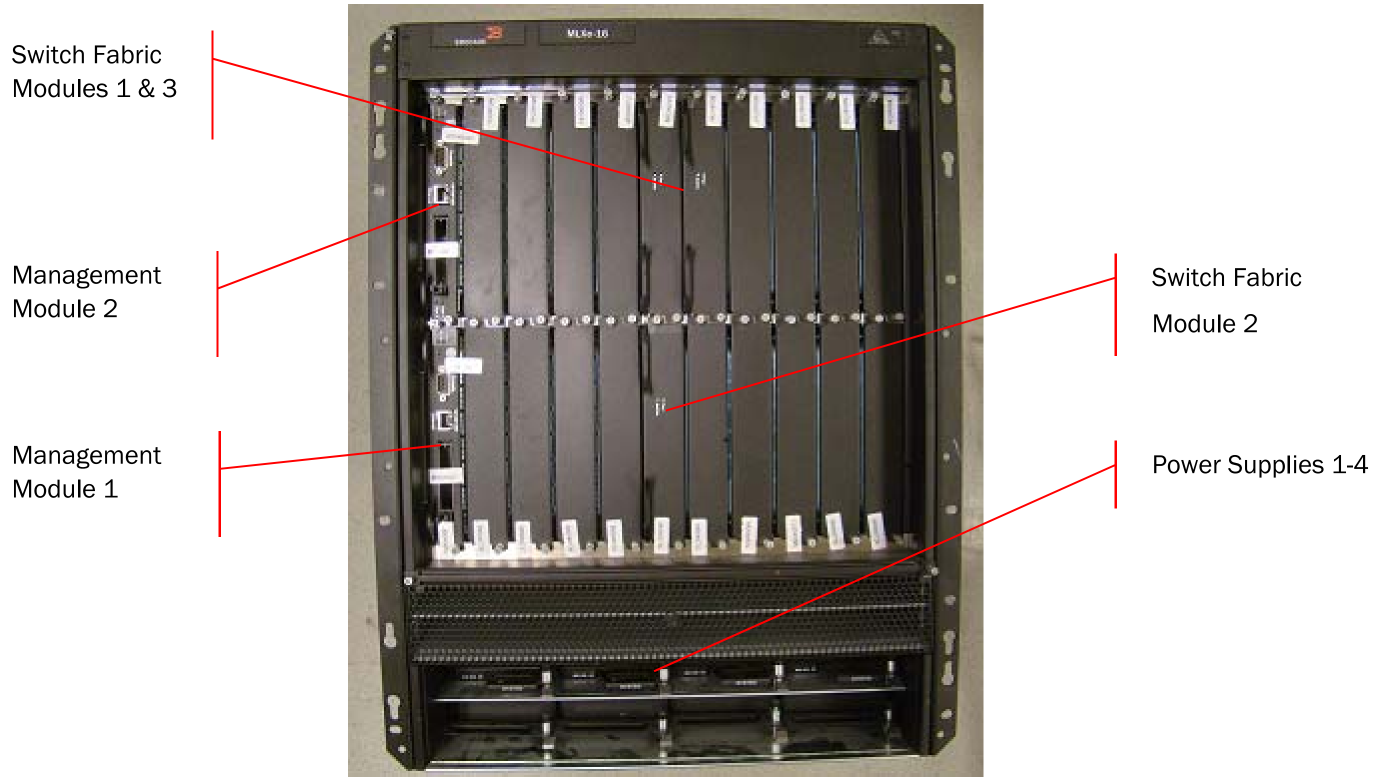
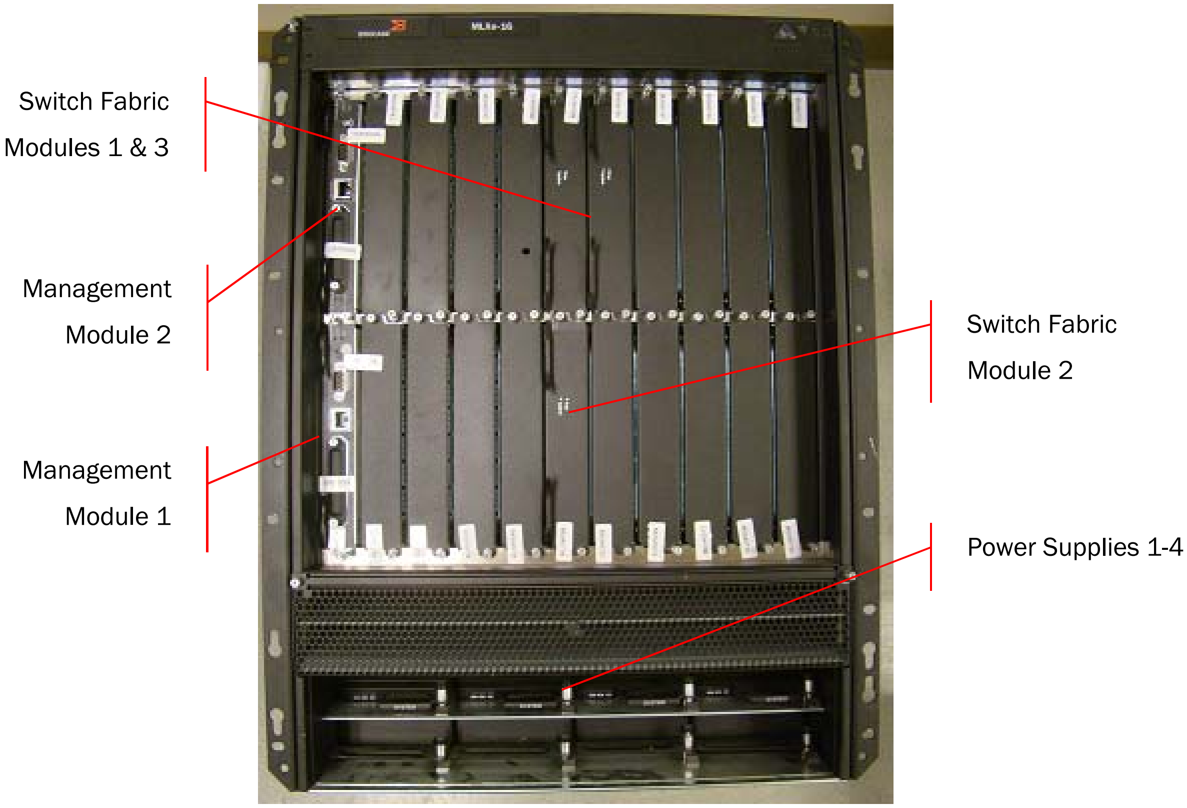


Figure 6 illustrates an MLXe-16 cryptographic module with two MR2 management modules. Table 8 defines the configuration of the validated MLXe-16 cryptographic module. Indicators are provided in Figure 6 to define the location of the management modules, switch fabric modules and power supply modules.

Figure 6 MLXe-16 Cryptographic Module with MR2 Management Modules



3 Brocade CER 2000 series

Table 9 CER 2000 Series Firmware Version

Firmware
IronWare Release R05.3.00ea
IronWare Release R05.4.00cb

Table 10 CER 2000 Series Part Numbers

SKU	MFG Part Number	Brief Description
NI-CER-2048F-ADVPREM-AC	80-1003769-07	NetIron CER 2048F includes 48 SFP ports of 100/1000 Mbps Ethernet. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software)
NI-CER-2048F-ADVPREM-DC	80-1003770-08	NetIron CER 2048F includes 48 SFP ports of 100/1000 Mbps Ethernet. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software)
NI-CER-2048FX-ADVPREM-AC	80-1003771-07	NetIron CES 2048FX includes 48 SFP ports of 100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software)
NI-CER-2048FX-ADVPREM-DC	80-1003772-08	NetIron CES 2048FX includes 48 SFP ports of 100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software)
NI-CER-2024F-ADVPREM-AC	80-1006902-02	NetIron CER 2024F includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W AC power supply (RPS9), and Advanced Services software
NI-CER-2024F-ADVPREM-DC	80-1006904-02	NetIron CER 2024F includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2024C-ADVPREM-AC	80-1007032-02	NetIron CER 2024C includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W AC power supply (RPS9), and Advanced Services software

SKU	MFG Part Number	Brief Description
NI-CER-2024C-ADVPREM-DC	80-1007034-02	NetIron CER 2024C includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2048C-ADVPREM-AC	80-1007039-02	NetIron CER 2048C includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. The router also includes 500W AC power supply (RPS9), and Advanced Services software
NI-CER-2048C-ADVPREM-DC	80-1007040-02	NetIron CER 2048C includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2048CX-ADVPREM-AC	80-1007041-02	NetIron CER 2048CX includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software
NI-CER-2048CX-ADVPREM-DC	80-1007042-02	NetIron CER 2048CX includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software

Table 11 CER Power Supply Module Part Numbers

SKU	MFG Part Number	Brief Description
RPS9	80-1003868-01	500W AC PWR SUPPLY FOR NI CER/CES SERIES
RPS9DC	80-1003869-02	500W DC PWR SUPPLY FOR NI CER/CES SERIES

Table 12 Validated CER 2000 Series Configurations

Validated CER 2000 Series Configurations	
CER Model	**SKUs (Count)**
NI-CER-2048F-ADVPREM-AC	Base: NI- CER-2048F-AC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9(1)
NI-CER-2048F-ADVPREM-DC	Base: NI-CER-2048F-DC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9DC(1)
NI-CER-2048FX-ADVPREM-AC	Base: NI-CER-2048FX-AC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9(1)
NI-CER-2048FX-ADVPREM-DC	Base: NI-CER-2048FX-DC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9DC(1)
NI-CER-2024F-ADVPREM-AC	Base: NI-CER-2024F-AC Interface module: None License: SW-CER-2024-ADVU (1) Power supply: RPS9(1)
NI-CER-2024F-ADVPREM-DC	Base: NI-CER-2024F-DC Interface module: None License: SW-CER-2024-ADVU (1) Power supply: RPS9DC(1)
NI-CER-2024C-ADVPREM-AC	Base: NI-CER-2024C-AC Interface module: None License: SW-CER-2024-ADVU (1) Power supply: RPS9(1)
NI-CER-2024C-ADVPREM-DC	Base: NI-CER-2024C-DC Interface module: None License: SW-CER-2024-ADVU (1) Power supply: RPS9DC(1)
NI-CER-2048C-ADVPREM-AC	Base: NI-CER-2048C-AC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9(1)
NI-CER-2048C-ADVPREM-DC	Base: NI-CER-2048C-DC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9DC(1)

Validated CER 2000 Series Configurations	
CER Model	**SKUs (Count)**
NI-CER-2048CX-ADVPREM-AC	Base: NI-CER-2048CX-ac Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9(1)
NI-CER-2048CX-ADVPREM-DC	Base: NI-CER-2048CX-DC Interface module: None License: SW-CER-2048-ADVU (1) Power supply: RPS9DC(1)

Figure 7 illustrates the CER 2024C cryptographic module.

Table 12 defines the configuration of the validated CER 2024C modules.

Figure 7 CER 2024C cryptographic module

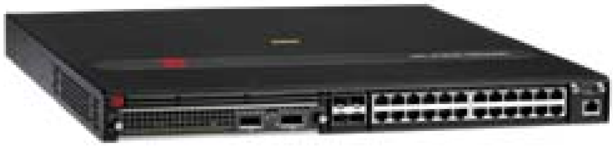


Figure 8 illustrates the CER 2024F cryptographic module.

Table 12 defines the configuration of the validated CER 2024F modules.

Figure 8 CER 2024F cryptographic module

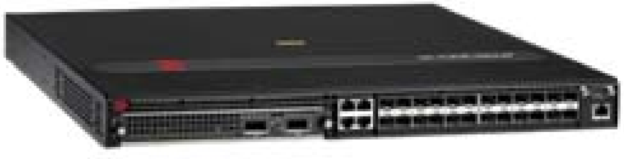


Figure 9 illustrates the CER 2048C cryptographic module.

Table 12 defines the configuration of the validated CER 2048C modules.

Figure 9 CER 2048C cryptographic module

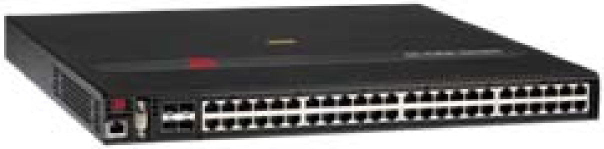


Figure 10 illustrates the CER 2048CX cryptographic module.

Table 12 defines the configuration of the validated CER 2048CX modules.

Figure 10 CER 2048CX cryptographic modules

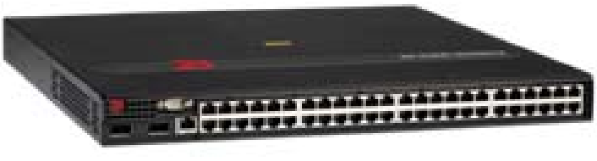


Figure 11 illustrates the CER 2048F cryptographic module.

Table 12 defines the configuration of the validated CER 2048F modules.

Figure 11 CER 2048F cryptographic modules

Figure 12 illustrates the CER 2048FX cryptographic module.

Table 12 defines the configuration of the validated CER 2048FX modules.

Figure 12 CER 2048FX cryptographic module

4 Ports and Interfaces

Each MLXe and CER device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces they provide for Data Input, Data Output, Control Input, and Control Output.

4.1.1 Brocade MLXe Series

While not included in this validation, the Brocade MLXe series supports a variety of interface modules. The Interface modules provide Ethernet ports with multiple connector types and transmission rates. Models in the series can provide up to:

- 256 10 Gigabit Ethernet ports per chassis
- 1536 Gigabit Ethernet ports per chassis,

See the *Interface modules section in* in [53-1002424-03] for supported interface modules, the ports each provides, and the corresponding status indicators.

4.1.2 MLXe MR and MR2 Management Cards

The MR management module provides physical ports and status indicators. The MR's major features are listed below.

- 1 GB SDRAM
- Dual PCMCIA slots for external storage.
- One Console port, EIA/TIA-232
- 10/100/1000 Mbps Ethernet port for out-of-band management.

The MR2 management module provides physical ports and status indicators. The MR2's major features are listed below.

- 4 GB SDRAM
- One internal 2GB compact flash drive
- One external compact flash slot
- Console port, EIA/TIA-232
- 10/100/1000 Mbps Ethernet port for out-of-band management

See the *Management Modules* section in [53-1002424-03] *for* detailed descriptions of management card ports and status indicators.

4.1.3 Brocade NetIron CER 2000 Series

Models in the Brocade NetIron CER 2000 series provide either 24 or 48 Gigabit Ethernet ports. The series supports both copper and fiber connecters with some models supporting combination ports. Some models support 10 Gigabit Ethernet uplink ports. All models have an out-of-band Ethernet management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

See the *Hardware Features* section in [53-1002425-03] for detailed descriptions of network ports (including combination ports), management ports, and status indicators provided by each model.

4.1.4 Interfaces

Table 13 shows the correspondence between the physical interfaces of NetIron devices and logical interfaces defined in FIPS 140-2.

Table 13 Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports	Data input
Console	
Networking ports	Data output
Console	
Networking ports	Control input
Console	
PCMCIA	
Networking ports	Status output
Console	
LED	
PCMCIA	
Power plugs	Power

4.1.4.1 Status LEDs

Table 14 Power and fan status LEDs for the CER 2024 models

LED	Position	State	Meaning
Fan (labeled Fn)	Right side of front panel	Green	The fan tray is powered on and is operating normal
		Amber or Green blinking	The fan tray is not plugged in.
		Amber	The fan tray is plugged in but one or more fans are faulty.
AC PS1 (labeled P1)	Right side of front panel	Off	Power supply 1 is not installed or is not providing power.
		Amber	Power supply 1 is installed, but not connected or a fault is detected.
		Green	Power supply 1 is installed and is functioning normally.
AC PS2 (labeled P2)	Right side of front panel	Off	Power supply 2 is not installed or is not providing power.
		Amber	Power supply 2 is installed, but not connected or a fault is detected.
		Green	Power supply 2 is installed and is functioning normally

Table 15 Power and fan status LEDs for the CER 2048 models[1]

LED	Position	State	Meaning
Fan (labeled Fn)	Left side of front panel	Green	The fan tray is powered on and is operating normal
		Amber or green blinking	The fan tray is not plugged in.
		Amber	The fan tray is plugged in but one or more fans are faulty.
PS1 (labeled P1)	Left side of front panel	Off	Power supply 1 is not installed or is not providing power.
		Amber	Power supply 1 is installed, but not connected or a fault is detected.
		Green	Power supply 1 is installed and is functioning normally.
PS2 (labeled P2)	Left side of front panel	Off	Power supply 2 is not installed or is not providing power.
		Amber	Power supply 2 is installed, but not connected or a fault is detected.
		Green	Power supply 2 is installed and is functioning normally
DC	Right side of front panel	Off	No DC Power
		Amber	The power supply has DC power, but the output is disabled or the power supply is over temperature or the fan failed

[1] The LEDs for the CER 2048CX, 2048F, and 2048FX models are just below the management Ethernet port on the left side of the front panel, labeled P1, P2, and Fn, left to right. The LEDs for the 2048C are just below the console connector on the left side of the front panel, labeled P1, P2, and Fn, left to right.

LED	Position	State	Meaning
		Green	Power supply has DC power, is enabled and is operating normal.
		Green blinking	Power supply has input power, but the DC output is disabled

Table 16 Power and fan status LEDs for the MR Management Module

LED	State	Meaning
Port 1 and Port 2	On or blinking	The software is currently accessing the auxiliary flash card
	Off	The software is not currently accessing the axillary flash card
Active	On	The module is functioning as the active management module
	Off	The module is functioning as the standby management module.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
10/100/1000 Ethernet Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
10/100/1000 Ethernet Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

Table 17 Power and fan status LEDs for the MR2 Management Module

LED	State	Meaning
Slot 1(Internal) and Slot 2(External)	On or blinking	The software is currently accessing the compact flash card
	Off	The software is not currently accessing the compact flash card
Active	On	The module is functioning as the active management module
	Off	The module is functioning as the standby management module.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
10/100/1000 Ethernet Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
10/100/1000 Ethernet Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

4.2 Modes of Operation

The NetIron cryptographic module can operate as a validated cryptographic module or non-validated cryptographic module. The factory default is to run the module as a non-validated module. Firmware integrity checks are always performed for the validated cryptographic module. Firmware integrity checks are not performed for the non-validated cryptographic module.

When the FIPS approved mode is invoked on a non-validated cryptographic module, the module starts operating as a validated cryptographic module. A validated cryptographic module cannot be transitioned to a non-validated cryptographic module.

The NetIron validated cryptographic module has two modes of operation: FIPS Approved mode and non-Approved mode. Section 6 describes services and cryptographic algorithms available in FIPS Approved mode. In non-Approved mode, the module runs without the FIPS operational rules applied. Section 8.1.1 FIPS Approved Mode describes how to invoke FIPS Approved mode.

The module does not support bypass.

4.3 Module Validation Level

The module meets an overall FIPS 140-2 compliance of security level 2 with Design Assurance level 3.

Table 18 NetIron Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Operational Environment	N/A

5 Roles

In FIPS Approved mode, NetIron devices support four roles: Crypto-officer, Port Configuration Administrator, User, and Unauthenticated:

1. Crypto-officer Role: The Crypto-officer role on the device in FIPS Approved mode is equivalent to administrator or super-user in non-Approved mode. Hence, the Crypto-officer role has complete access to the system.
2. Port Configuration Administrator Role: The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-Approved mode. Hence, the Port Configuration Administrator role has read-and-write access for specific ports but not for global (system-wide) parameters.
3. User Role: The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).
4. Unauthenticated Role: The unauthenticated role on the device in FIPS Approved mode is possible while using serial console to access the device. Console is considered as a trusted channel. The scope of the role is same as the User Role without authentication. The enable command allows user to authenticate using a different role. Based on the authentication method mentioned in Section 6.1, the role would change to one of Crypto-officer, Port Configuration Administrator or User role.

The User role has read-only access to the cryptographic module while the Crypto-officer role has access to all device commands. NetIron modules do not have a maintenance interface.

For MLXe devices see the *Assigning Permanent Passwords* section of Chapter 6 – Connecting a Router to a Network Device in [53-1002424-03] and Chapter 2 – Securing Access to Management Functions, in [53-1002423-02] for details on role capabilities.

For CER devices see the *Permanent Assignment* section of Chapter 2 – Connecting a Brocade Device to a Network Device in [53-1002425-03] and Chapter 2 – Securing Access to Management Functions, in [53-1002423-02] for details on role capabilities.

Within this document, Section 7.2 Authentication describes the authentication policy for the user roles.

6 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-test by power cycling a NetIron device.

For all other services, an operator must authenticate to the device as described in Section 7.2 Authentication.

NetIron devices provide services for remote communication (SSH, SCP, HTTPS, SNMPv3 and Console) for management and configuration of cryptographic functions. Per IG D.8 scenario 4, SSH, TLS and SNMPv3 KDFs are allowed to be used in FIPS mode but are non-compliant. Hereafter this non-compliance applies to all references to SSH, TLS and SNMPv3.

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameter (CSP) associated with the service. Table 19 summarizes the available FIPS Approved cryptographic functions. Table 20 lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

Table 19 FIPS Approved Cryptographic Functions

Label	Cryptographic Function
AES	Advanced Encryption Algorithm
Triple-DES	Triple Data Encryption Algorithm
SHA	Secure Hash Algorithm
HMAC	Keyed-Hash Message Authentication code
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
RSA	Rivest Shamir Adleman Signature Algorithm

Table 20 Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

Label	Cryptographic Functions
KW	RSA Key Wrapping
DH	Diffie-Hellman key agreement
SNMP	SNMPv3
MD5	Message-Digest algorithm 5
KDF	SSHv2 and TLS Key Derivation Function

6.1 User Role Services

The User management privilege level allows access to the User EXEC, and Privileged EXEC commands, but only with read access. See the EXEC commands section of the Brocade MLX Series and NetIron Family Configuration Guides, [53-1002423-02] and [53-1002544-02] for further information on scope of User EXEC, and Privileged EXEC commands.

6.1.1 SNMP

The SNMP service within the User Role allows read-only access to the SNMP MIB within the NetIron device, using SNMPv1, v2c or v3 versions. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for read-only access (status output).

6.1.2 Console

Console connections occur via a directly connected RS-232 serial cable. Once authenticated in the User role, the module provides console commands to display information about a NetIron device and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available are same as the list mentioned in the SSH service.

6.2 Port Configuration Administrator Role Services

The Port Configuration Administrator management privilege level allows read-and-write access for port configuration, but not for global (system-wide) parameters.

6.2.1 SNMP

Section 6.1.3, above, describes this service.

The SNMP service is not available for the Port Configuration Administrator role.

6.2.2 Console

Section 6.1.4, above, describes this service.

Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. The commands available to operator within the Port Configuration Administrator role are same as those mentioned in the SSH service Section 6.2.1.

6.3 Crypto-officer Role Services

The Crypto-officer management privilege level allows complete read-and-write access to the system. This is generally for system administrators and is the only management privilege level that allows one to configure passwords.

6.3.1 SNMP

Section 6.1.3, above, describes this service.

The SNMP service within Crypto-officer role allows access to the SNMP MIB within the NetIron device as per the capability of the SNMP agent, using SNMPv1, v2c or v3 versions. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for access similar to non-Approved mode of operation.

6.3.2 Console

This service is described in Section 6.1.4 above.

Console commands provide an authenticated Crypto-officer complete access to all the commands within the NetIron device. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSH service, the operator would create a pair of DSA or RSA host keys and configure the authentication scheme for SSH access. To enable the Web Management service, the operator would create a pair of RSA host keys and a digital certificate using corresponding commands, and enable the HTTPS server.

6.4 Non-Approved Mode Services

Certain services are available within the non-Approved mode of operation, which are otherwise not available in the FIPS Approved mode of operation. They are:

6.4.1 SSH

This service provides a secure session between a NetIron device and an SSH client. The NetIron device authenticates an SSH client and provides an encrypted communication channel. An operator may use an SSH session for managing the device via the command line interface.

NetIron devices support three kinds of SSH client authentication: password, keyboard interactive and public-key authentication.

For password authentication, an operator attempting to establish an SSH session provides a password through the SSH client. The NetIron device authenticates operator with passwords stored on the device, on a TACACS or TACACS+ server, or on a RADIUS server. Section 7.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one-step ahead. It allows multiple challenges to be issued by the NetIron device, using the backend RADIUS or TACACS+ server, to the SSH client. Only after the SSH client responds correctly to the challenges, will the SSH client get authenticated and proper access is given to the NetIron device.

For public key authentication, possession of a private key serves as an authentication method. In PKI (Public Key Infrastructure), each private key has its corresponding public key and they are referred as a key pair. Every key pair is unique. The cryptographic module uses a database of client public keys and its associated user names and roles to support public key authentication. The SSH client which possesses the private key sends a signature (over some data from the request including the user name) created using the private key. The cryptographic module uses the public key corresponding to the user and verifies the signature to authenticate the user.

In the User Role, the client is given access to three commands: enable, exit and terminal. The enable command allows the operator to reauthenticate using a different role. If the role is the same, based on the credentials given during the enable command, the operator has access to a small subset of commands that can perform ping, traceroute, outbound SSH client in addition to show commands.

6.4.2 HTTPS

This service provides a graphical user interface for managing a NetIron MLXe device over a secure communication channel. The HTTPS service is not supported on CER 2000 Series devices. Using a web browser, an operator connects to a designated TCP port on a NetIron device. The device negotiates a TLS connection with the browser and authenticates the operator. The device uses HTTP over TLS with cipher suites TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA

In the User role, after a successful login, the default HTML page is same for any role. The operator can surf to any page after clicking on any URL. However, this operator is not allowed to make any modifications. If the user presses the ‘Modify’ button within any page, the user will be challenged to reenter the crypto-officer’s credentials. The challenge dialog box does not close unless the operator provides the crypto-officer’s access credentials. After three failed attempts, the page ‘Protected Object’ is displayed, in effect disallowing any changes from the web.

6.4.3 SCP

This is a secure copy service that works over SSH protocol. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary files can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and data compression level configured for SSH. For example, if password authentication is enabled for SSH, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on NetIron devices is to copy user digital certificates and host public-private key pairs to the cryptographic module in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

6.4.4 TFTP

Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user.

6.4.5 Telnet

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

6.4.6 SNMP

Allows access to Critical Security Parameter (CSP) MIB objects

6.4.7 HTTP

This service provides a graphical user interface for managing a NetIron MLXe device over an unsecure communication channel. The HTTP service is not supported on CER 2000 Series devices.

7 Policies

7.1 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 2 security requirements. After configuring a NetIron device to operate in FIPS Approved mode the Crypto-officer must execute the "fips self-tests" command to validate the integrity of the firmware installed on the device. If an error is detected during the self-test, the error must be corrected prior to rebooting the device. See Section 7.1.1.1 and Section 7.1.1.2 for further details.

1) The cryptographic module provides role-based authentication.
2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSP).
3) The cryptographic module performs the following tests:
    a) Power up Self-Tests:
        i) Cryptographic Known Answer Tests (KAT):
            (1) RC2 40 bit key size KAT (encrypt/decrypt)
            (2) RC4 40 bit key size KAT (encrypt/decrypt)
            (3) DES 56 bit key size KAT (encrypt/decrypt)
            (4) Triple-DES-56bit key size KAT (encrypt/decrypt)
            (5) AES-128,192,256-bit key sizes KAT (encrypt/decrypt)
            (6) MD2 KAT (Hashing)
            (7) MD5 KAT (Hashing)
            (8) SHA-1,256,384,512 KAT (Hashing)
            (9) HMAC-SHA-1,256,384,512 KAT (Hashing)
            (10) RSA 2048 bit key size KAT (encrypt/decrypt)
            (11) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature/verification)
            (12) DSA 1024 bit key size, SHA-1 KAT (signature/verification)
            (13) DRBG KAT
        ii) Firmware Integrity Test[2] (DSA 1024 bit, SHA-1 Signature Verification)
        iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

Crypto module initialization and Known Answer Test (KAT) Passed.

[2] The firmware integrity test is performed only when the device is configured to run in FIPS Approved mode.

iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

Crypto Module Failed <Reason String>

b) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on non-Approved RNG.

ii) Continuous Random Number Generator test – performed on DRBG.

iii) RSA 1024/2048 SHA-1 Pairwise Consistency Test (Sign/Verify)

iv) RSA 1024/2048 Pairwise Consistency Test (Encrypt/Decrypt)

v) DSA 1024 SHA-1 Pairwise Consistency Test (Sign/Verify)

vi) Bypass Test: N/A

vii) Manual Key Entry Test: N/A

4) At any time the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the "fips self-tests" command.

5) Data output to services defined in Section 6 Services is inhibited during key generation, self-tests, zeroization, and error states.

6) Status information does not contain CSPs or sensitive data that if used could compromise the module.

7.1.1 Cryptographic Module Operational Rules

In order to operate an MLXe and CER 2000 series device securely, an operator should be aware of the following rules for FIPS Approved mode of operation.

External communication channels/ports are not be available before initialization of an MLXe and CER 2000 series device.

MLXe and CER 2000 series devices use a FIPS Approved random number generator implementing Algorithm Hash DRBG based on hash functions.

MLXe and CER 2000 series ensures that the random number seed and seed key input do not have same value. The devices generate seed keys and do not accept a seed key entered manually.

MLXe and CER 2000 series devices test the prime numbers generated for both DSA and RSA keys using Miller-Rabin test. See [RSA PKCS #1] Appendix 2.1 A Probabilistic Primality Test.

MLXe and CER 2000 series devices use non-approved key establishment techniques:

- Diffie-Hellman
- RSA Key Wrapping

MLXe and CER 2000 series devices restrict key entry and key generation to authenticated roles.

MLXe and CER 2000 series devices do not display plaintext secret or private keys. The device displays "…" in place of plaintext keys.

MLXe and CER 2000 series devices use automated methods to realize session keys for SSHv2 and HTTPS.

MLXe and CER 2000 series devices perform Get, GetNext, GetBulk and Set SNMP operations. Neither device provides SNMP access to CSPs when operating in FIPS Approved mode.

7.2 Authentication

NetIron devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS/TACACS+, RADIUS and local configuration database. Moreover, NetIron supports multiple authentication methods for each service.

To implement one or more authentication methods for securing access to the device, an operator in the Crypto-officer role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (SSH, Web, SNMP, and so on) and the order in which the device tries one or more of the following authentication methods:

1. Line password authentication,
2. Enable password authentication,
3. Local user authentication,
4. RADIUS authentication with exec authorization and command authorization, and
5. TACACS/TACACS+ authentication with exec authorization and command authorization

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a TACACS+ server) the device tries the next method until a method in the list is available or all methods have been tried.

NetIron devices allow multiple concurrent operators through SSH and the console. One operator's configuration changes can overwrite the changes of another operator. See [53-1002423-02] *Single user in CONFIG mode*.

7.2.1 Line Authentication Method

The line method uses the Telnet password to authenticate an operator.

To use line authentication, a Crypto-officer must set the Telnet password. See *Setting the Telnet password* in [53-1002423-02]. Please note that when operating in FIPS Approved mode, Telnet is disabled and Line Authentication is not available.

7.2.2 Enable Authentication Method

The enable method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-config password to the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto-officer Role.

To use enable authentication, a Crypto-officer must set the password for each privilege level. See *Setting passwords for management privilege levels* in [53-1002423-02].

7.2.3 Local Authentication Method

The local method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The NetIron device assigns the role associated with the user name to the operator when authentication is successful.

To use local authentication, a Crypto-officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role). See *Setting up local user accounts* in [53-1002423-02].

7.2.4 RADIUS Authentication Method

The RADIUS method uses one or more RADIUS servers to verify user names and passwords. The NetIron device prompts an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server does not respond, the NetIron device will send the user name and password information to the next configured RADIUS server.

NetIron series devices support additional command authorization with RADIUS authentication. The following events occur when RADIUS command authorization takes place.

1. A user previously authenticated by a RADIUS server enters a command on the NetIron device.
2. The NetIron device looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3. If the command belongs to a privilege level that requires authorization, the NetIron device looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the NetIron device. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the NetIron device.

To use RADIUS authentication, a Crypto-officer must configure RADIUS server settings along with authentication and authorization settings. See *RADIUS configuration procedure* in [53-1002423-02].

7.2.5 TACACS/TACACS+ Authentication Method

The TACACS and TACACS+ methods use one or more TACACS/TACACS+ servers to verify user names and passwords. For TACACS, the NetIron device prompts an operator for user name and password. The device sends the user name and password to the TACACS server. Upon successful authentication, the NetIron device selects the operator's role implicitly based on the action requested (for example, User role is selected for a login request and Crypto-officer role is selected for a configure terminal command). For TACACS+ authentication, the NetIron device prompts an operator for a user name, which the device uses to get a password prompt from the TACACS+ server. The operator enters a password, which the device relays to the server for validation. Upon successful authentication, the TACACS+ server supports both exec and command authorization similar to RADIUS authorization described above.

To use TACACS/TACACS+ authentication, a Crypto-officer must configure TACACS/TACACS+ server settings along with authentication and authorization settings. See *TACACS configuration procedure* and *TACACS+ configuration procedure* in [53-1002423-02].

7.2.6 Strength of Authentication

NetIron devices minimize the likelihood that a random authentication attempt will succeed. The probability that a random guess of a password will succeed is less than 1 in 10,000,000. The probability of a successful random guess of a password during a one-minute period is less than 6 in 1,000,000.

7.3 Access Control and Critical Security Parameter (CSP)

Table 21 Access Control Policy and Critical Security Parameter (CSP) summarize the access operators in each role have to critical security parameters. Grayed out table cells indicate that the intersection of the role the CSP have not security relevance. The table entries have the following meanings:

- r – operator can read the value of the item,
- w – operator can write a new value for the item,
- x – operator can use the value of the item (for example encrypt with an encryption key), and
- d – operator can delete the value of the item by executing a fips zeroize all command. See item 3a in Section 8.1.1.1 and Section 8.1.1.2 for further details.

Table 21 Access Control Policy and Critical Security Parameter (CSP) for Approved Services

	User	Port Administrator	Crypto-officer
Service CSP	Console	Console	Console
SSH host RSA or DSA private key			wd
SSH host RSA or DSA public key			rwd

	User	Port Administrator	Crypto-officer
Service CSP	Console	Console	Console
SSH client RSA or DSA public key			xrwd
SSH session key			
TLS host RSA private key			wd
TLS host RSA digital certificate			rwd
TLS pre-master secret			
TLS session key			
TLS authentication key			
DH Private Exponent			
DH Public Key			
User Password	x		xrwd
Port Administrator Password		x	xrwd
Crypto-officer Password			xrwd
RADIUS Secret	x	x	xrwd
TACACS+ Secret	x	x	xrwd
Firmware Integrity DSA public key			x
DRBG Seed			
DRBG Value V	x	x	x
DRBG Constant C	x	x	x
Hash DRBG Entropy	x	x	x

Table 22 Access Control Policy and Critical Security Parameter (CSP) for Non-Approved Services

	User			Port Administrator		Crypto-officer			
Service / CSP	SSH	HTTPS	SNMP	SSH	HTTPS	SSH	SCP	HTTPS	SNMP
SSH host RSA or DSA private key	x			x		xwd	x		
SSH host RSA or DSA public key	x			x		xrwd	xrw		
SSH client RSA or DSA public key	x			x		xrwd	xrwd		
SSH session key	x			x		x	x		
TLS host RSA private key		x			x	wd		x	
TLS host RSA digital certificate		x			x	rwd		x	
TLS pre-master secret		x			x			x	
TLS session key		x			x			x	
TLS authentication key		x			x			xd	
DH Private Exponent	x			x		x	x		
DH Public Key	x			x		x	x		
User Password	x	x	x			xrwd	xrwd	xrwd	x
Port Administrator Password				x	x	xrwd	xrwd	xrwd	
Crypto-officer Password						xrwd	xrwd	xrwd	
RADIUS Secret	x	x		x	x	xrwd	xrwd	xrwd	
TACACS+ Secret	x	x		x	x	xrwd	xrwd	xrwd	
Firmware Integrity DSA public key						x		x	
DRBG Seed	x	x		x	x	x	x	x	
DRBG Value V	x	x	x	x	x	x	x	x	x
DRBG Constant C	x	x	x	x	x	x	x	x	x
Hash DRBG Entropy	x	x	x	x	x	x	x	x	x

7.3.1 CSP Zeroization

The SSH session key is transient. It is zeroized at the end of a session and recreated at the beginning of a new session.

The TLS pre-master secret is generated during the TLS handshake. It is destroyed after it is used.

The TLS session key is generated for every HTTPS session. The TLS session key is deleted after the session is closed.

The DRBG seed and Hash DRBG Entropy is recomputed periodically on 100 millisecond intervals. Each time this occurs, four bytes of the seed are written into an 8K buffer. When the buffer is full the DRBG V and C values are regenerated and the buffer is zeroized.

The DH private exponent is generated at the beginning of DH KEX. A new random number overwrites the memory location used to store the value each time a new session is initiated.

The Firmware Integrity DSA public key cannot be written, read or deleted. The key pair is prebuilt within the code binary. The key pair is destroyed and recreated each time new firmware is installed.

For SSH, the RSA private key is stored in a locally generated file on flash during the key generation process. The file is removed during zeroization. The *crypto key zeroize* command removes the keys.

Executing the *no fips enable* command zeroizes all host key pairs

7.4 Physical Security

NetIron devices require the Crypto-officer to install tamper evident labels (TELs) in order to meet FIPS 140-2 Level 2 Physical Security requirements. The TELs are available from Brocade under part number XBR-00195. The Crypto-officer shall follow the Brocade FIPS Security Seal application procedures prior to operating the module in FIPS Approved mode. The FIPS seal application procedure is available in Appendix A

8 Crypto-officer Guidance

For each module to operate in a FIPS Approved mode of operation, the tamper evident seals supplied in Brocade XBR-000195 must be installed, as defined in Appendix A.

The security officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The security officer shall maintain a serial number inventory of all used and unused tamper evident seals. The security officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The security officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The security officer is responsible for returning a module to a FIPS Approved state after any intentional or unintentional reconfiguration of the physical security measures.

The Brocade MLX Series and NetIron Family Configuration Guide [53-1002423-02] and Brocade MLX Series and NetIron Family Federal Information Processing Standards Guide [53-1002735-02]. In particular, the NetIron family FIPS guide provides configuration instructions specific to operating a NetIron devices in FIPS Approved mode.

8.1 Mode Status

NetIron devices provide the fips show command to display status information about the device's configuration. This information includes the status of administrative commands for security policy, the status of security policy enforcement, and security policy settings. The fips enable command changes the status of administrative commands; see also Section 8.1.1 FIPS Approved Mode.

The following example shows the output of the fips show command before an operator enters a fips enable command. Administrative commands for security policy are unavailable (administrative status is off) and the device is not enforcing a security policy (operational status is off).

```
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

The following example shows the output of the fips show command after an operator enters the fips enable command. Administrative commands for security policy are available (administrative status is on) but the device is not enforcing a security policy yet (operational status is off). The command displays the security policy settings.

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be FIPS 140-2 compliant and have to be
zeroized separately by the Crypto-officer before the system is rebooted. This ensures that the data path of
the system is not immediately impacted after FIPS Approved mode is enabled administratively. A separate
command needs to be executed by the Crypto-officer in order to zeroize all the configured shared secrets
and keys.
The system needs to be reloaded to operationally enter FIPS Approved mode.
System Specific:
OS monitor mode access:                                   Disabled
Management Protocol Specific:
Telnet server:                                            Disabled
TFTP Client:                                              Disabled
HTTPS SSL 3.0:                                            Disabled
SNMP Access to security objects:                          Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:                Clear
SSH DSA Host Keys:                                        Clear
HTTPS RSA Host Keys and Signature:                        Clear
```

The status ‘Clear’ refers to the fact that when FIPS Approved mode is disabled at a later point in time, the corresponding CSPs will be affected based on the FIPS policy settings for that CSP.

The following example shows the output of the fips show command after the device reloads successfully in the default strict FIPS Approved mode. Administrative commands for security policy are available (administrative status is on) and the device is enforcing a security policy (operational status is on): The command displays the policy settings.

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access:                                   Disabled
Management Protocol Specific:
Telnet server:                                            Disabled
TFTP Client:                                              Disabled
HTTPS SSL 3.0:                                            Disabled
SNMP Access to security objects:                          Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:                Clear
SSH DSA Host Keys:                                        Clear
HTTPS RSA Host Keys and Signature:                        Clear
```

8.1.1 FIPS Approved Mode

This section describes the FIPS Approved mode of operation and the sequence of actions that put a NetIron device in FIPS Approved mode. FIPS Approved mode disables the following:

1. Telnet access including the telnet server command
2. AAA authentication for the console including the enable aaa console command
3. Command ip ssh scp disable
4. TFTP access
5. SNMP access to CSP MIB objects
6. Access to all commands within the monitor mode
7. HTTP access including the web-management http command (applies to Brocade MLXe series only)
8. HTTPS SSL 3.0 access and RC4 cipher (applies to Brocade MLXe series only)
9. Command web-management allow-no-password (applies to Brocade MLXe series only)

Entering FIPS Approved mode also clears:

1. Protocol shared secret and host passwords
2. SSH DSA host keys
3. HTTPS RSA host keys and certificate (applies Brocade MLXe series only)

FIPS Approved mode enables:

1. SCP
2. HTTPS TLS version 1.0 and greater (applies to Brocade MLXe series only)

In FIPS Approved mode, NetIron devices provide FIPS Approved cryptographic algorithms as well as non-Approved security functions.

Table 23 Algorithm Certificates for the MLXe Series with an MR Management Module

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128-, 192, and 256-bit keys, ECB and CBC mode	2359
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	1475
Secure Hash Algorithm	SHA-1, SHA-256, SHA-384, and SHA-512	2031
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1462
Deterministic Random Bit Generator (DRBG)	SHA-256 Based SP 800-90 DRBG	301
Digital Signature Algorithm (DSA)	1024-bit keys	737*
Rivest Shamir Adleman Signature Algorithm (RSA)	1024-bit and 2048-bit keys	1217*

Table 24 Algorithm Certificates for the MLXe Series with an MR2 Management Module

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128-, 192, and 256-bit keys, ECB and CBC mode	2359
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	1475
Secure Hash Algorithm	SHA-1, SHA-256, SHA-384, and SHA-512	2031

Algorithm	Supports	Certificate
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1462
Deterministic Random Bit Generator (DRBG)	SHA-256 Based SP 800-90 DRBG	301
Digital Signature Algorithm (DSA)	1024-bit keys	737*
Rivest Shamir Adleman Signature Algorithm (RSA)	1024-bit and 2048-bit keys	1217*

Table 25 Algorithm Certificates for the CER 2000 Series

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128-, 192, and 256-bit keys, ECB and CBC mode	2359
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	1475
Secure Hash Algorithm	SHA-1, SHA-256, SHA-384, and SHA-512	2031
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1462
Deterministic Random Bit Generator (DRBG)	SHA-256 Based SP 800-90 DRBG	301
Digital Signature Algorithm (DSA)	1024-bit keys	737*
Rivest Shamir Adleman Signature Algorithm (RSA)	1024-bit and 2048-bit keys	1217*

*Note: RSA(Cert. #1217; non-compliant with the functions from the CAVP Historical RSA list)

FIPS186-2:
ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024 , 1536 , SHS: SHA-1, SHA-256, SHA-384, SHA-512, 2048 , 3072 , 4096 , SHS: SHA-1

DSA(Cert. #737; non-compliant with the functions from the CAVP Historical DSA list)

FIPS186-2:
PQG(gen) MOD(1024);
KEYGEN(Y) MOD(1024);
SIG(gen) MOD(1024);

The following non-Approved but allowed cryptographic methods are allowed within limited scope in the FIPS Approved mode of operation:

1. SNMPv3 (Cryptographic function does not meet FIPS requirements and is considered plaintext)
2. MD5 – Used in the TLS v1.0 pseudo-random function (PRF) in FIPS mode (MD5 not exposed to the operator). Also used in TACACS+ packets for message integrity verification (MD5 not exposed to the operator).
3. HMAC-MD5 – Used to support RADIUS authentication
4. SSHv2 and TLS Key Derivation Function (KDF) - This is a legacy implementation.
5. HMAC-SHA1-96 [RFC 2404] is used for IPSec ESP Authentication header [RFC 4835], which is used for OSPFv3 authentication [RFC 4552].

The following non-Approved and not allowed cryptographic methods are not allowed within limited scope in the FIPS Approved mode of operation:

1. RSA Key Wrapping [Non Compliant]
2. Diffie-Hellman (DH) [Non Compliant]
3. DES
4. MD2
5. RC2
6. RC4

8.1.1.1 Invoking FIPS Approved Mode for Brocade MLXe Series Devices

To invoke the FIPS Approved mode of operation, perform the following steps from the console terminal.

1. Assume Crypto-officer role
   a. The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in section 7.2 Authentication. Both the Enable Authentication Method and Local Authentication Method can be used to assume the Crypto-officer role.
2. Copy signature files of all the affected images to the flash memory as per the Brocade MLX Series and NetIron Family Federal Information Processing Standards Guide [53-1002735-02],
3. Enter command: fips enable
   a. The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do *not* change the default strict FIPS security policy, which is required for FIPS Approved mode.
4. Enter command: fips zeroize all
   a. The device zeros out the shared secrets use by various networking protocols including host access passwords, SSH host keys, and HTTPS host keys with the digital signature.
5. Save the running configuration: write memory
   a. The device saves the running configuration as the startup configuration
6. Enter command: fips self-tests
   a. This command validates the cryptographic module by running Known Answer Tests (KAT), Conditional Tests and the Firmware Integrity test described in Section 7.1 Security Rules. Pay careful attention to the output, especially the Firmware Integrity test. If there are any missing or mismatch signature files on the flash, this test will provide more details. The Crypto-officer may have to copy signature files to take corrective action.
   b. This command could be executed again and corrective actions needs to be taken until the output does not give any more error indication. Without this action, the Power-On Self-Test will fail after reload is performed and the cryptographic module will go in continuous reload state as is required in FIPS mode of operation.
7. Reload the device
   a. The device resets, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
8. Enter command: fips show
   a. The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
9. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

8.1.1.2 Invoking FIPS Approved Mode for Brocade NetIron CER 2000 Series Devices

To invoke the FIPS Approved mode of operation, perform the following steps from the console terminal.

1. Assume Crypto-officer role

2. Copy signature files of all the affected images to the flash memory as per the Brocade MLX Series and NetIron Family Federal Information Processing Standards Guide [53-1002735-01].
3. Enter command: fips enable
    a. The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do *not* change the default strict FIPS security policy, which is required for FIPS Approved mode.
4. Enter command: fips zeroize all
    a. The device zeros out the shared secrets used by various networking protocols including host access passwords, SSH host keys, and HTTPS host keys with the digital signature.
5. Save the running configuration: write memory
6. The device saves the running configuration as the startup configuration
7. Enter command: fips self-tests
    a. This command validates the cryptographic module by running Known Answer Tests (KAT), Conditional Tests and Firmware Integrity test as described in Section 7.1 Security Rules. Pay careful attention to the output, especially the Firmware Integrity test. If there are any missing or mismatch signature files on the flash, this test will provide more details. The Crypto-officer may have to copy signature files to take corrective action.
    b. This command could be executed again and corrective actions needs to be taken until the output does not give any more error indication. Without this action, the Power-On Self-Test will fail after reload is performed and the cryptographic module will go in continuous reload state as is required in FIPS Approved mode of operation.
8. Reload the device
    a. The device resets, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
9. Enter command: fips show
    a. The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
10. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

8.1.1.3 Negating FIPS Approved Mode for Brocade MLXe Series Devices

To exit the FIPS Approved mode of operation, perform the following steps from the console terminal.

1. Enter command: no fips enable
    a. This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, HTTP, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.
    b. The device zeroes out the shared secrets used by various networking protocols including host access passwords, SSH host keys, and HTTPS host keys with the digital signature.
    c. Reload the device to begin non-Approved mode of operation.

8.1.1.4 Negating FIPS Approved Mode for Brocade CER 2000 Series Devices

To exit the FIPS Approved mode of operation, perform the following steps from the console terminal.

1. Enter command: no fips enable
    a. This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.

b. The device zeroes out the shared secrets used by various networking protocols including host access passwords, SSH host keys, and HTTPS host keys with the digital signature.

c. Reload the device to begin non-Approved mode of operation.

9 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CER	Carrier Ethernet Router
CLI	Command Line Interface
CFP	C Form-factor Pluggable
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
ECDSA	Elliptic Curve Digital Signature Algorithm
FI	FastIron platform
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
LP	Line Processor
Mbps	Megabits per second
MP	Management Processor
NDRNG	Non-Deterministic Random Number Generator
NI	NetIron platform
OC	Optical Carrier
PRF	pseudo-random function
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SFP	Small Form-factor Pluggable
SFPP	Small Form-factor Plus Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SSH	Secure Shell
TACACS	Terminal Access Control Access-Control System
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
XFP	10 Gigabit Small Form Factor Pluggable

10 References

[53-1002423-02] Brocade MLX Series and NetIron Family Configuration Guide, Supporting Multi-Service IronWare R05.3.00a, Brocade Communications Systems, Inc., Publication number 53-1002423-02, 16 April 2012

[53-1002424-03] Brocade MLX Series and NetIron XMR Hardware Installation Guide, Supported Release: Multi-Service IronWare R05.3.00a, Brocade Communications Systems, Inc., Publication Number 53-1002424-03, 14 May 2012

[53-1002425-03] Brocade NetIron CES 2000 and NetIron CER 2000 Hardware Installation Guide, Supported Release: Multi-Service IronWare R05.3.00a, Brocade Communications Systems, Inc., Publication number 53-1002425-03, 31 May 2012

[53-1002735-01] Brocade MLX Series and NetIron Family Federal Information Processing Standards Guide, Supporting Multi-Service IronWare R05.3.00, Brocade Communications Systems, Inc., Publication number 53-1002735-01, 31 August 2012

[53-1002544-02] Brocade MLX Series and NetIron Family Configuration Guide, Supporting Multi-Service IronWare R05.4.00a, Brocade Communications Systems, Inc., Publication number 53-1002544-01, 25 September 2012

[53-1002545-02] Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide, Supported Release: Multi-Service IronWare R05.4.00a, Brocade Communications Systems, Inc., Publication number 53-1002545-01, 25 September 2012

[53-1002546-02] Brocade NetIron CES and Brocade NetIron CER Devices Hardware Guide, Supported Release: Multi-Service IronWare R05.4.00a, Brocade Communications Systems, Inc., Publication number 53-1002546-01, 25 September 2012

[53-1002805-01] Brocade MLX Series and NetIron Family Documentation Updates, Supporting Multi-Service IronWare R05.4.00b, Brocade Communications Systems, Inc., Publication number 53-1002805-01, 19 December 2012

[53-1002962-01] Brocade MLX Series and NetIron Family Federal Information Processing Standards Guide, Supporting Multi-Service IronWare R05.4.00, Brocade Communications Systems, Inc., Publication number 53-1002962-01, 05 June 2013

[FIPS 186-2+] Federal Information Processing Standards Publication 186-2 (+Change Notice), Digital Signature Standard (DSS), 27 January 2000

[RSA PKCS #1] PKCS #1: RSA Cryptography Specifications Version 2.1, http://tools.ietf.org/html/rfc3447

[SP800-90] National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007

Appendix A: Tamper Label Application

The FIPS Kit (SKU XBR-000195) contains the following items:

- Tamper Evident Security Seals
  - Count 120
  - Checkerboard destruct pattern with ultraviolet visible "Secure" image
- 53-1002458-02 : FIPS Pointer Document Guideline
  - This document provides instructions on how to access the [53-1002118-02] FIPS Security Seal Procedures for Brocade MLXe Series and Brocade NetIron CER 2000 Series, document on the MyBrocade website.

Use 99% isopropyl alcohols to clean the surface area at each tamper evident seal placement location. Isopropyl alcohol is not provided in the kit. However, 99% isopropyl alcohol is readily available for purchase from a chemical supply company. Prior to applying a new seal to an area, that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use additional alcohol to clean off any residual adhesive remover before applying a new seal.

Applying Evident Seals to a Brocade MLXe-4 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-4 device. Each Brocade MLXe-4 device requires the placement of seventeen seals:

Front: Thirteen seals are required to complete the physical security requirements illustrated in Figure 13. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

Rear: Four seals are required to complete the physical security requirements illustrated in Figure 14. Affix one seal at each location designated in Figure 14. Each seal is applied from the top panel of the chassis to the flange of each of the four fan FRUs. You must bend each seal to place them correctly. See Figure 14 for correct seal orientation and positioning.

Figure 13 Front view of a Brocade MLXe-4 device with security seals

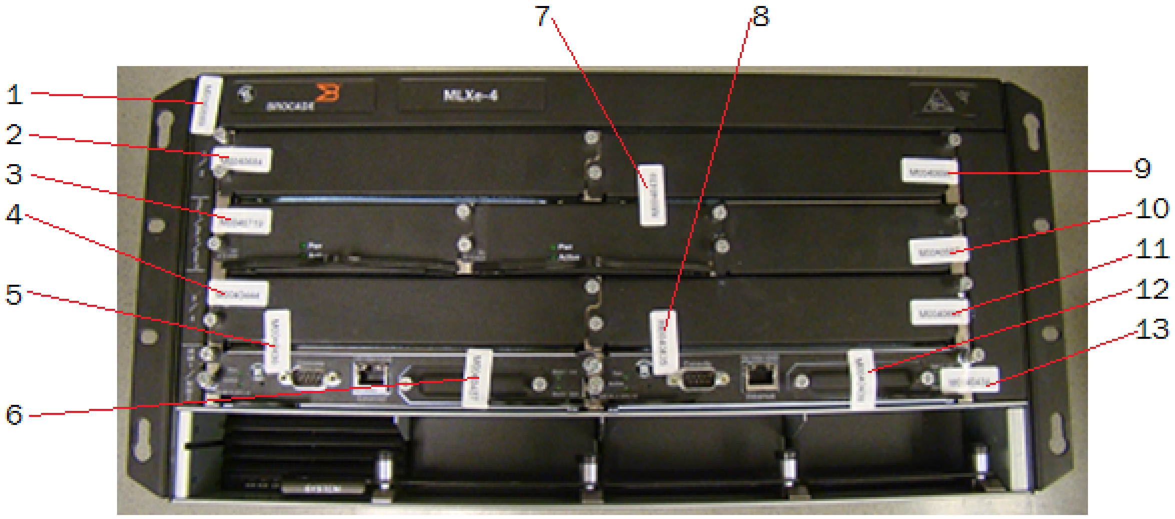
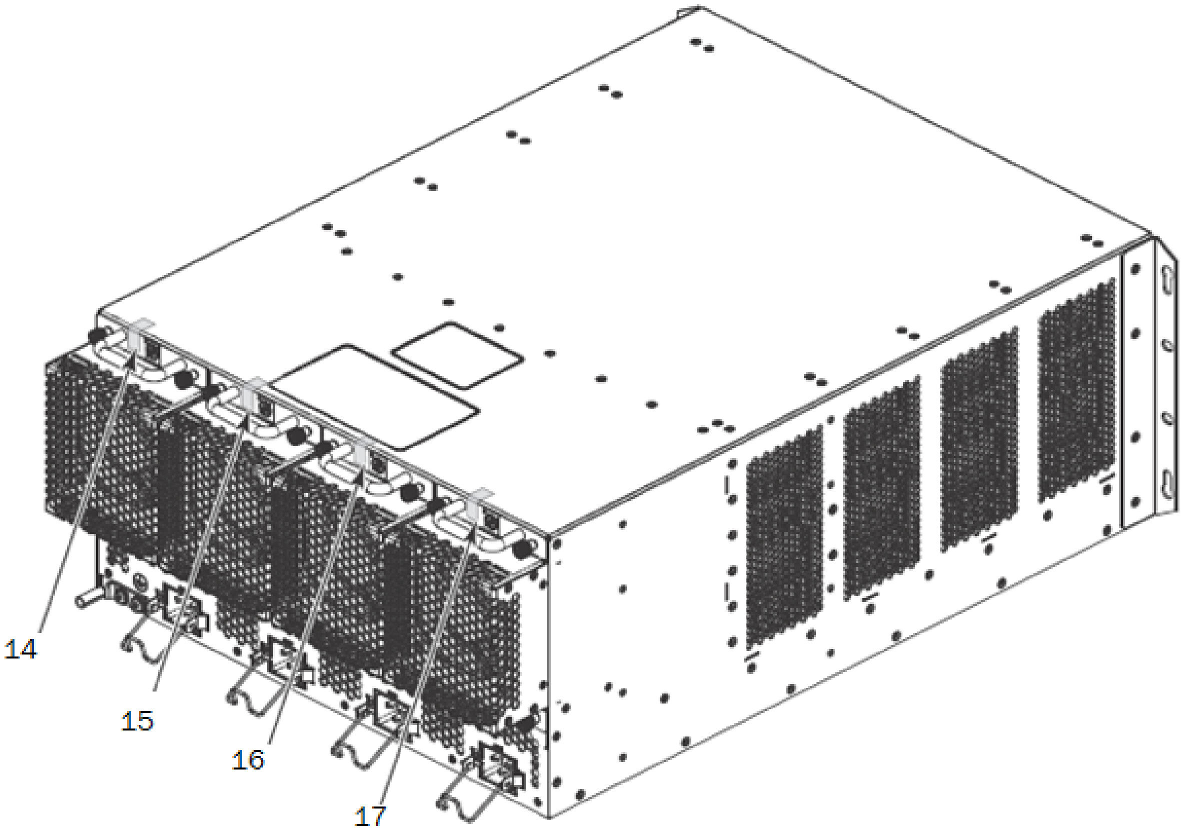


Figure 14 Rear and side view of a Brocade MLXe-4 device with security seals



Applying Evident Seals to a Brocade MLXe-8 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-8 device. Each Brocade MLXe-8 device requires the placement of twenty seals:

Front: Eighteen seals are required to complete the physical security requirements illustrated in Figure 15. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

Rear: Two seals are required to complete the physical security requirements illustrated in Figure 16. Affix one seal at each location designated in Figure 16. Each seal is applied from the top panel of the chassis to the flange of each of the two fan FRUs. You must bend each seal to place them correctly. See Figure 16 for correct seal orientation and positioning.

Figure 15 Front view of a Brocade MLXe-8 device with security seals

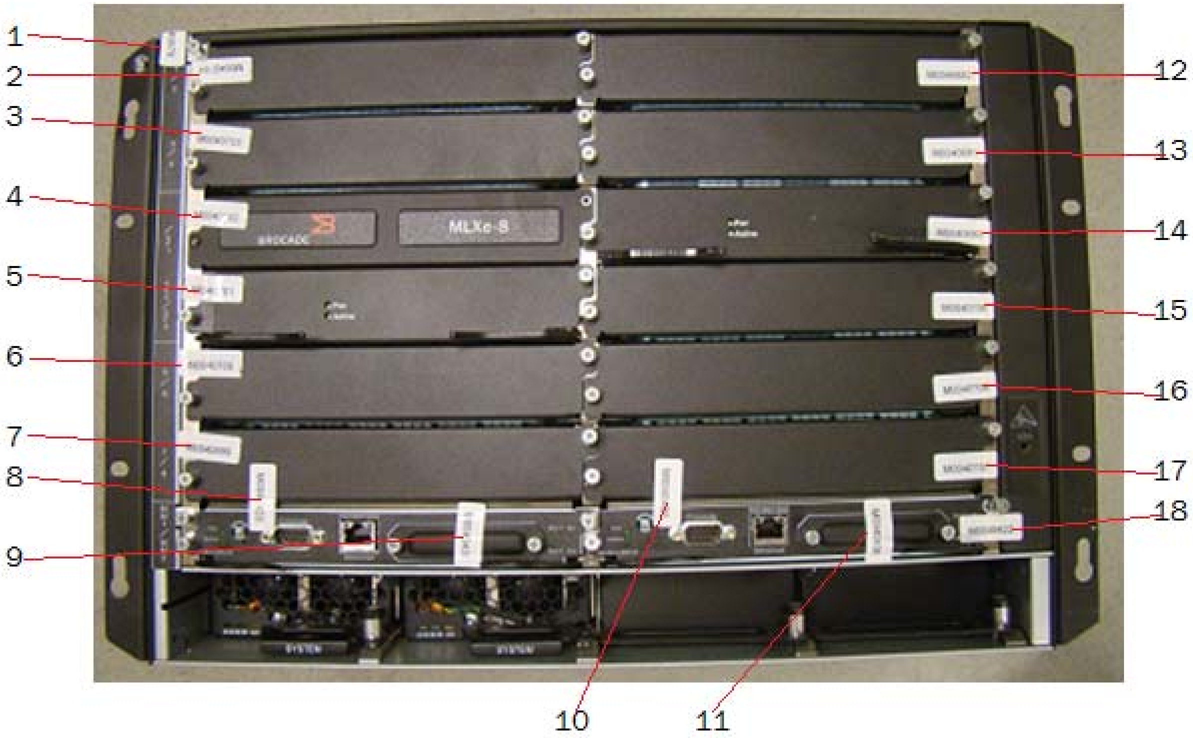
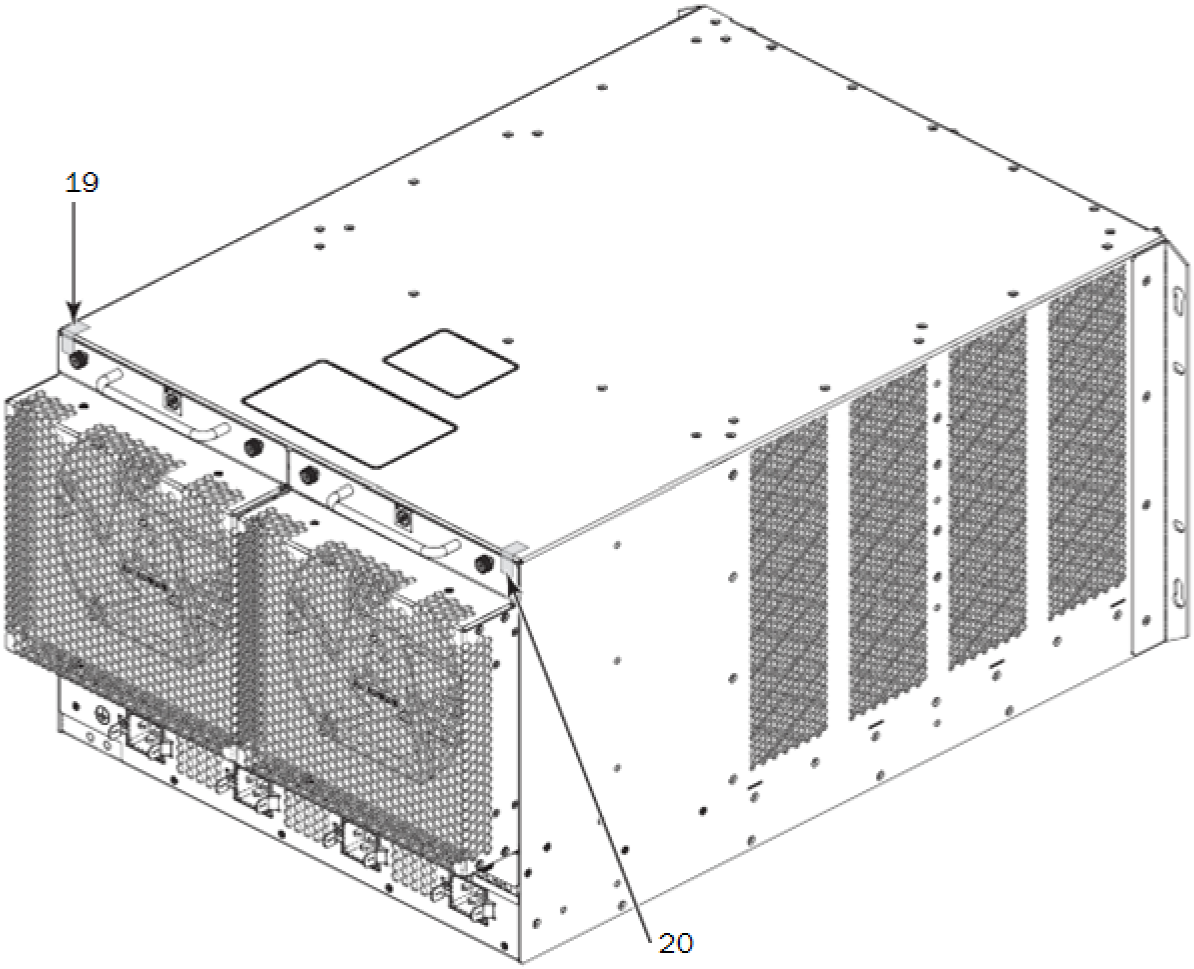


Figure 16 Rear and side view of a Brocade MLXe-8 device with security seals



Applying Evident Seals to a Brocade MLXe-16 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-16 device. Each Brocade MLXe-16 device requires the placement of twenty-seven seals:

Front: Twenty-five seals are required to complete the physical security requirements illustrated in Figure 17. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

Rear: Two seals are required to complete the physical security requirements illustrated in Figure 18. Affix one seal at each location designated in Figure 18. Each seal is applied from the back panel of the chassis to the flange of each of the two fan FRUs. See Figure 18 for correct seal orientation and positioning.

Figure 17 Front view of a Brocade MLXe-16 device with security seals

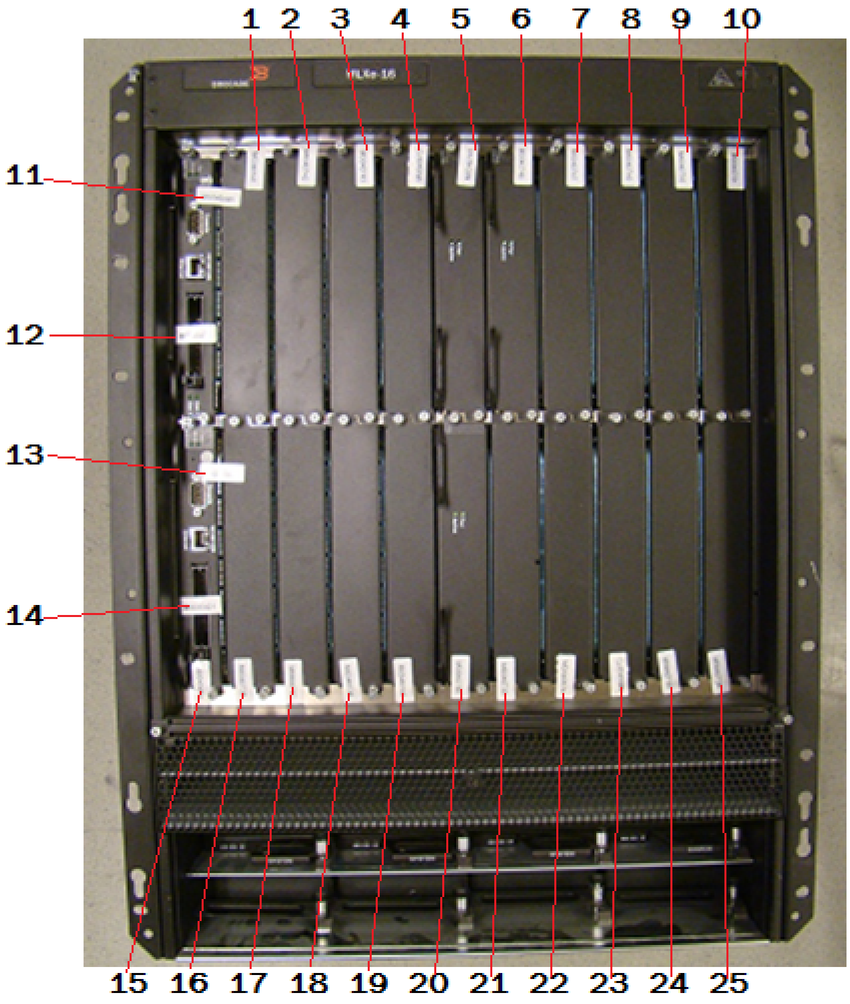
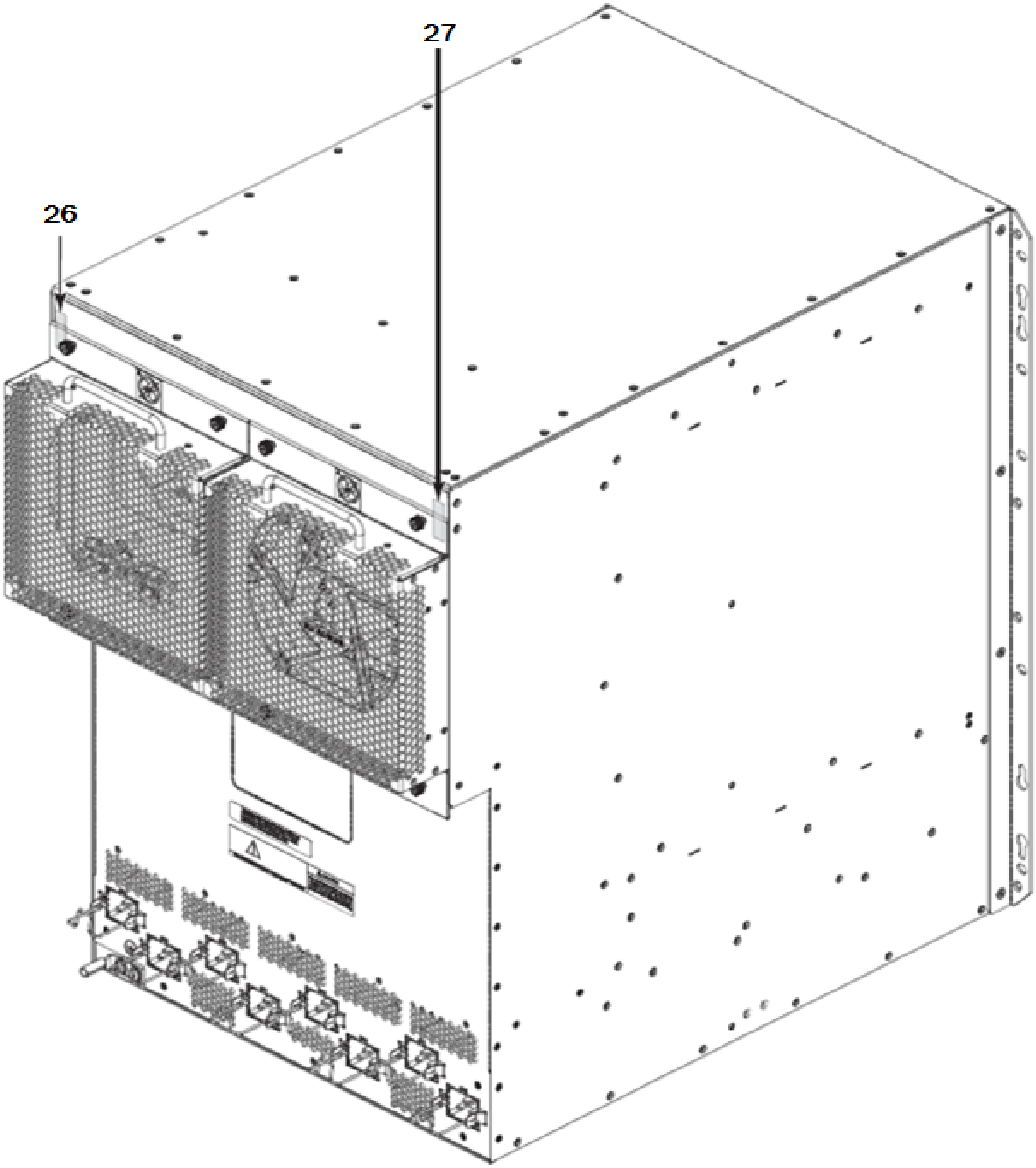


Figure 18 Rear and side view of a Brocade MLXe-16 device with security seals



Applying Evident Seals to Brocade NetIron CER 2024 devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CER 2024C and CER 2024F devices. The connectors on the faceplate of a particular model may vary, but the placement of the seals is the same.

Brocade NetIron CER 2024C and CER 2024F devices require the placement of 21 seals:

- Top: Affix one seal lengthwise completely covering the top rightmost screw that connects the faceplate to the device. See Figure 19 for correct seal orientation and positioning.
- Right and left sides: Affix seven seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 19 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side. See Figure 20 for correct seal orientation and positioning on the left side.
- Front: Affix a seal from the front panel to the bottom panel. See Figure 19 for correct seal orientation and placement.
- Rear: Affix four seals from the top panel to the rear panel. Affix one seal from the rear panel to the bottom panel. See Figure 20 for correct seal orientation and placement.

Figure 19 Front, top, and right side view of a Brocade NetIron CER 2024 device with security seals

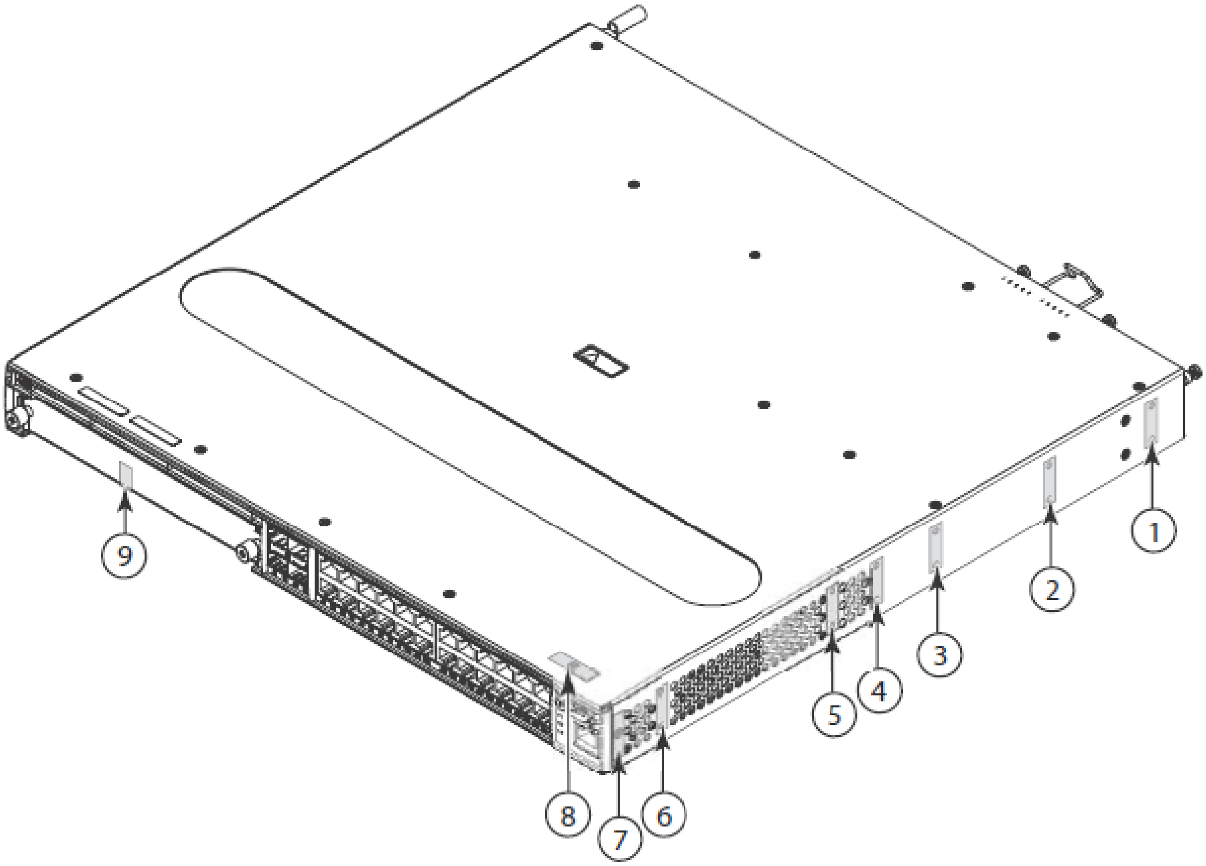
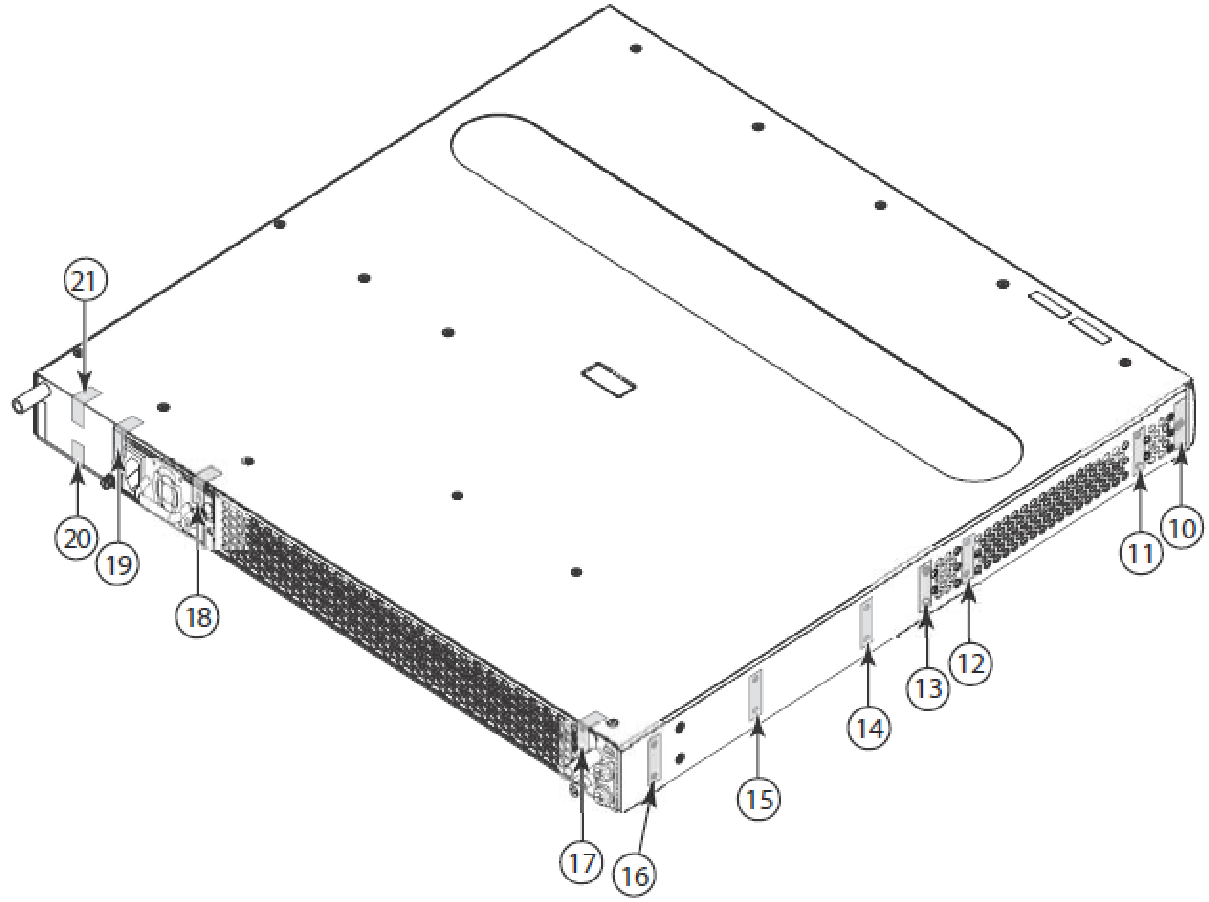


Figure 20 Rear, top and left side view of a Brocade NetIron CER 2024 device with security seals



Applying Evident Seals to a Brocade NetIron CER 2048 devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CER 2048C and CER 2048F series devices. The connectors on the faceplate of a particular model may vary, but the placement of the seals is the same.

Brocade NetIron CER 2048C, Brocade NetIron CER 2048CX, Brocade NetIron CER 2048F and Brocade NetIron CER 2048FX devices require the placement of 20 seals:

- **Top**: Affix one seal lengthwise completely covering the top rightmost screw that connects the faceplate to the device. See Figure 21 for correct seal orientation and positioning.
- **Right and left sides**: Affix seven seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 21 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side. See Figure 22 for correct seal orientation and positioning on the left side.
- **Rear**: Affix four seals from the top panel to the rear panel. Affix one seal from the rear panel to the bottom panel. See Figure 22 for correct seal orientation and placement

Figure 21 Front, top, and right side view of a Brocade NetIron CER 2048 device with security seals

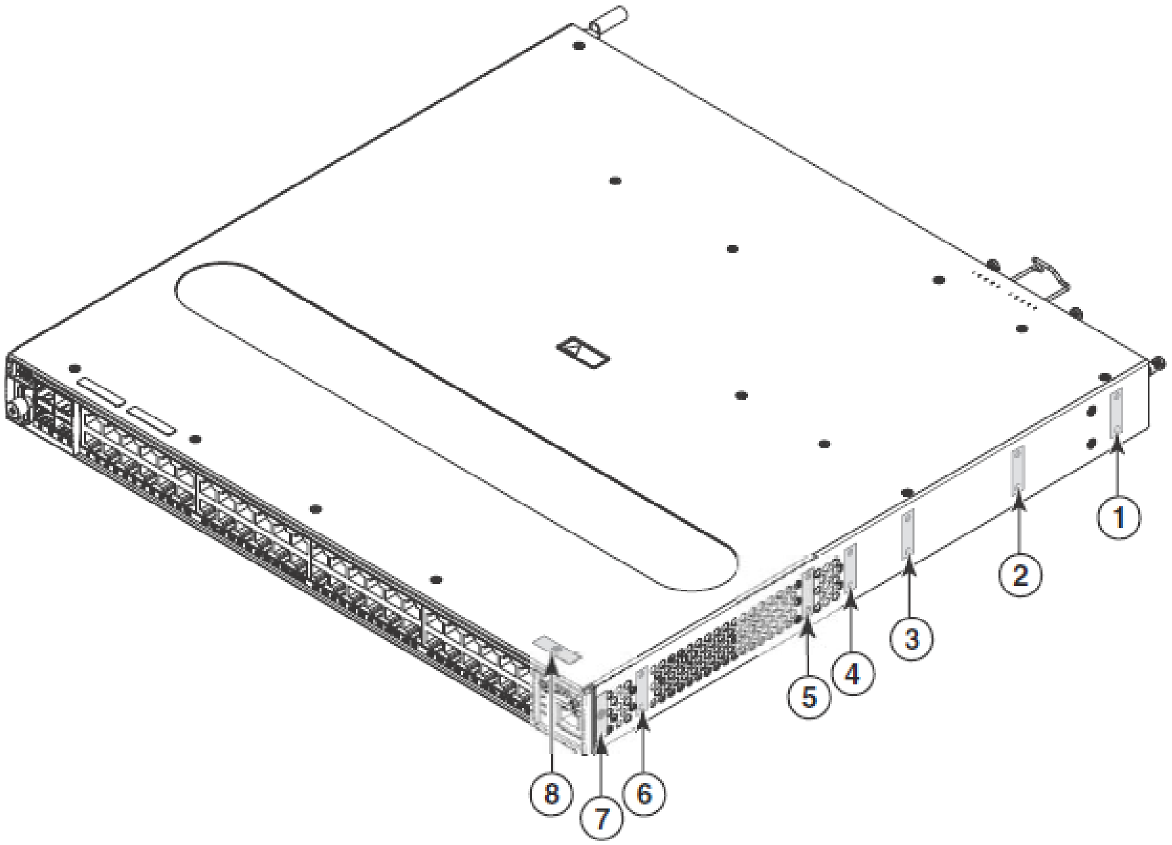
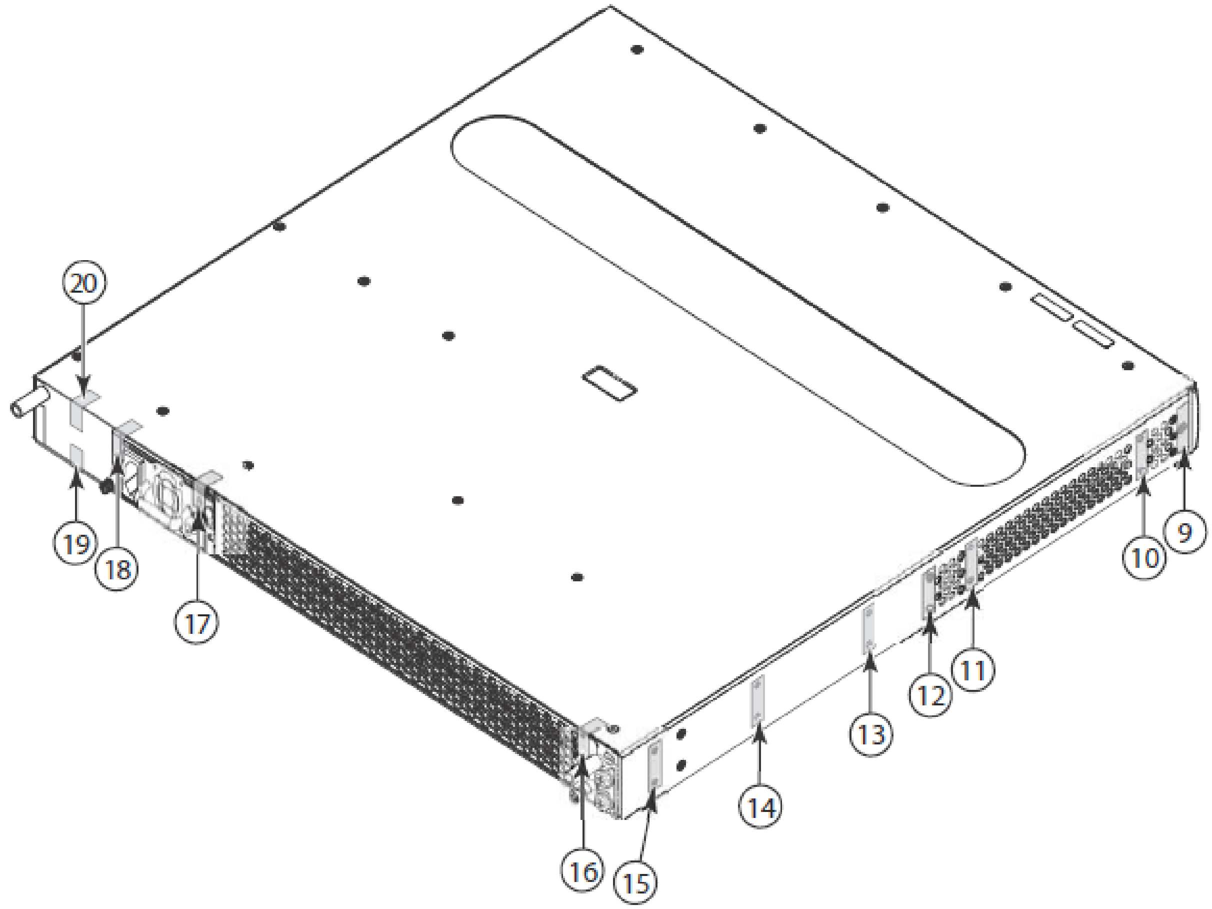


Figure 22 Rear, top and left side view of a Brocade NetIron CER 2048 device with security seals


20
19
18
17
16
15
14
13
12
11
10
9