Brocade ICX 6430 and ICX 6450 Series Stackable Switch with FastIron 7.4.00a Firmware

FIPS 140-2 Non-Proprietary Security Policy

Level 2 with Design Assurance Level 3 Validation

Document Version 0.5

November 20, 2013

Revision History

Revision Date	Revision	Summary of Changes
11/20/2013	0.5	Initial release

© 2013 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, MLX, SAN Health, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Contact a Brocade sales office for information on feature and product availability.

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

Tables

Figures

1 Introduction

Brocade® ICX™ 6430 and 6450 switches provide enterprise-class stackable LAN switching solutions to meet the growing demands of campus networks. Designed for small to medium-size enterprises, branch offices, and distributed campuses, these intelligent, scalable edge switches deliver enterprise-class functionality without compromising performance and reliability.

2 Overview

The FIPS140-2 validation includes the eight hardware devices presented in Table 2 running the firmware version presented in Table 1, referred collectively for the remainder of this document as ICX 6430/6450 device (cryptographic module, or simply the module). Each ICX 6430/6450 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. Four models are available in both the ICX 6430 series and ICX 6450 series. The power supplies and fan tray assemblies are part of the cryptographic boundary and cannot be replaced in the field. The cryptographic boundary for each ICX 6430 or ICX 6450 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident seals, supplied in FIPS Kit (Part Number: Brocade XBR-000195) must be installed, as defined in Appendix A.

2.1 FastIron Firmware

The ICX 6430 series and ICX 6450 series (listed in Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers) run the same firmware version that includes the cryptographic functionality described in Section 4

Table 1 Firmware Version

Firmware Version
FI 7.4.00a

2.2 ICX 6430 and ICX 6450 Series

Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers

	SKU	MFG Part Number	Brief Description
#1	ICX 6430-24	80-1006002-02	24-port 1G Switch, 4 x 1G SFP Uplink/Stacking Ports
#2	ICX 6430-24P	80-1006000-02	24-port 1G Switch PoE+ 390W, 4 x 1G SFP Uplink/Stacking Ports
#3	ICX 6430-48	80-1006003-02	48-port 1G Switch, 4 x 1G SFP Uplink/Stacking Ports
#4	ICX 6430-48P	80-1006001-02	48-port 1G Switch PoE+ 390W, 4 x 1G SFP Uplink/Stacking Ports
#5	ICX 6450-24	80-1005997-02	24-port 1G Switch, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
#6	ICX 6450-24P	80-1005996-02	24-port 1G Switch PoE+ 390W, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
#7	ICX 6450-48	80-1005999-03	48-port 1G Switch, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
#8	ICX 6450-48P	80-1005998-02	48-port 1G Switch PoE+ 780W, 2x1G SFP+ (upgradable to 10G) & 2x1G/10G SFP+ Uplink/Stacking Ports
#1 to #8 above with	XBR-000195	NA	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Label Application in this document.

Figure 1 illustrates the ICX 6430-24 and ICX 6430-24P cryptographic modules (#1 and #2 in Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers).

Figure 1 ICX 6430-24 and ICX 6430-24P cryptographic modules

Figure 2 illustrates the ICX 6430-48 and ICX 6430-48P cryptographic modules (#3 and #4 in Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers).

Figure 2 ICX 6430-48 and ICX 6430-48P cryptographic modules

Figure 3 illustrates the ICX 6450-24 and ICX 6450-24P cryptographic module (#5 and #6 in Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers)

Figure 3 ICX 6450-24 and ICX 6450-24P cryptographic module

Figure 4 illustrates the ICX 6430-48 and ICX 6430-48P cryptographic modules (#7 and #8 in Table 2 ICX 6430 and ICX 6450 Switch Family Part Numbers).

Figure 4 ICX 6450-48 and ICX 6450-48P cryptographic modules

2.3 Ports and Interfaces

Each ICX 6430 and ICX 6450 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.

While not part of this validation, the ICX 6430 and ICX 6450 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

Tables 3 and 4 summarize the physical ports provided by the ICX 6430 and ICX 6450 models. Tables , 5 and 6 show the correspondence between the physical interfaces of an ICX 6430 and ICX 6450 device and the logical interfaces defined in FIPS 140-2.

Table 3 ICX 6430 Port mapping to logical interface

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
External power supply connector (ICX 6430-24P, ICX 6430-48 and ICX 6430-48P only)	Power
Out of band management port	Control input, Status output
Console Port	Control input, Status output
Reset	Control input
LED	Status output

Table 4 ICX 6450 Port mapping to logical interface

Physical Port	Logical Interface
SFP/SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
External power supply connector (EPS) (The ICX 6450-24, ICX 6450-24P and ICX 6450-48 have one EPS connector. The ICX 6450-48P has two EPS connectors	Power
Out of band management port[i]	Control input, Status output
Console Port	Control input, Status output
Reset	Control input
LED	Status output

Table 5 ICX 6430 and ICX 6450 Series Physical Port LED Status

LED	Condition	Status
Ethernet Ports 24-port and 48-port models	On/Flashing Green	The port has established a valid link at 10, 100 or 1000 Mbps. Flashing indicates the port is transmitting and receiving user packets
	Off	A link is not established with a remote port.

LED	Condition	Status
PoE/PoE+ 24-port and 48-port models	On/Green	The port is providing PoE or PoE+ power to a connected device.
	Off	The port is not providing PoE or PoE+ power.
SFP/SFP+ (X1 - X4) for ICX 6450 devices	On/Flashing Green	The SFP port is operating at 10 Gbps. Flashing indicates the port is transmitting and receiving user packets at 10 Gbps.
	On/Flashing Yellow	The SFP port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
	Off	A link is not established with a remote port.
SFP (F1 - F4) for ICX 6430 devices	On/ Flashing Green	The SFP port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
	Off	A link is not established with a remote port.
Out-of-band management port (2 LEDs)	Off (both LEDs)	Offline
	On/Flashing (left side)	Link-up. Flashing indicates the port is transmitting and receiving user packets.
	On/Green (right side)	1 Gbps Link-up
	Right LED off, left LED on or flashing	10/100 Mbps Link-up. Flashing indicates the port is transmitting and receiving user packets.

Table 6 ICX 6430 and ICX 6450 System LED Status

LED	Condition	Status
EPS1 and EPS2 (External Power Supply status for ICX 6450-48P devices only)	Green	EPS1 and EPS2 power supplies are operating normally.
	Yellow	EPS1 and EPS2 power supply fault
	Off	EPS1 and EPS2 off or not present
PWR (Power)	Green	Power supply is operating normally.
	Yellow	Power supply fault
	Off	Power supply off..
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Yellow	System self-diagnostic test has detected a fault. (Fan, thermal, or any interface fault.) The user must reload the system..
MS (Stacking configuration)	Green	The device is the Active controller. Flashing indicates the system is initializing.
	Yellow	Indicates the device is the Standby controller. Flashing indicates the system is in Master arbitration or selection state.
	Off	Device is operating as a stack member, or is in standalone mode.
Uplink (X1 and X2 stacking port status)	Green	Uplink port is operating normally.
	Off	Uplink failed or there is not link.
Downlink	Green	Downlink port is operating normally.

LED	Condition	Status
(X3 and X4, stacking port status)	Off	Downlink failed or there is not link.
1-8 (Switch ID in the stack)	Green	Indicates the switch ID in the stack. For ICX 6430 devices, 1 - 4 indicates the switch ID in the stack. For ICX 6450 devices, 1 - 8 indicates the switch ID in the stack.

2.4 Modes of Operation

The ICX 6430/6450cryptographic module has two modes of operation: FIPS Approved mode and non-FIPS Approved mode. Section 4 describes services and cryptographic algorithms available in FIPS-Approved mode. In non-FIPS Approved mode, the module runs without these FIPS policy rules applied. Section 5.5.1 FIPS Approved Mode describes how to invoke FIPS-Approved mode.

2.5 Module Validation Level

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

Table 7 ICX 6430/6450 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
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Roles

In FIPS Approved mode, ICX 6430/6450 supports three roles: Crypto Officer, Port Configuration Administrator, and User:

1. Crypto Officer Role (Super User): The Crypto Officer role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode the Crypto Officer role has complete access to the system.
2. Port Configuration Administrator Role (Port Configuration): The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-FIPS 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 (Read Only): The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

The User role has read-only access to the cryptographic module while the Crypto Officer role has access to all device commands. ICX 6430/6450 modules do not have a maintenance interface or maintenance role.

Section 5.2 Authentication describes the authentication policy for user roles.

4 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 determine if the network connections are functioning properly. Unauthenticated operators can also perform self-test via power-cycle. They can also view the module status via "fips show".

For all other services, an operator must authenticate to the device as described in section 5.2 Authentication.

ICX 6430/6450 devices provide services for remote communication (SSHv2, Secure Web Management over TLS v1.0, SNMPv3 and Console) for management and configuration of cryptographic functions.

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSP) associated with the service. "Table 8 FIPS Approved Cryptographic Functions" summarizes the available FIPS-Approved cryptographic functions. "Table 9 FIPS Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode" lists cryptographic functions that while not FIPS-Approved are allowed in FIPS Approved mode of operation.

Table 8 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
ECDSA	Elliptic Curve Digital Signature Algorithm
RSA	Rivest Shamir Adleman Signature Algorithm

Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

Table 9 FIPS Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

Label	Cryptographic Functions
KW	RSA Key Wrapping
DH KA	Diffie-Hellman key agreement
SNMP	SNMPv3 (considered as plaintext; uses the following algorithms: AES-128-CFB (non-compliant); SHS (non-compliant); HMAC-SHA-1 (non-compliant); DES; MD5; HMAC-MD5)
MD5	
KDF	SSHv2 Key Derivation Function
HWRNG	Generation of seeds for DRBG

Table 10 FIPS Non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode

Label/Protocol	Cryptographic Functions
HTTPS Cipher Suites	RSA_WithDES_CBC_SHA RSA_With3DES_EDE_CBC_SHA DHE_DSSWithDES_CBC_SHA DHE_DSSWith3DES_EDE_CBC_SHA DHE_RSAWithDES_CBC_SHA DHE_RSAWith3DES_EDE_CBC_SHA RSA_Export1024WithDES_CBC_SHA RSA_WithAES_128_CBC_SHA RSA_WithAES_256_CBC_SHA DHE_DSS_WITH_AES_128_CBC_SHA DHE_RSA_WITH_AES_128_CBC_SHA DHE_DSS_WITH_AES_256_CBC_SHE_RSA_WITH_AES_256_CBC_SHA
HTTP	None
SNMP (Simple Network Management Protocol v1 and v2)	None
TACACS	HMAC-MD5
TFTP (Trivial File Transfer Protocol)	None
“Two way encryption”	None; Base64
MD5	Message Digest 5
Syslog	None
OSPF[1]-IPSEC	IPSEC Authentication only; none
VSRP	None
VRRP/VRRP-E	None
MPLS RSVP	None
MPLS-LDP	None
MSTP	None
SNTP	None
NTP	None
FCSP	None
BGP	None
Key Generation	RSA

[1] *Open Shortest Path First*

4.1 User Role Services

4.1.1 SSH

This service provides a secure session between an ICX 6430/6450 device and a SSH client using SSHv2 protocol. The ICX 6430/6450 device authenticates a SSH client and provides an encrypted communication channel. An operator may use a SSH session for managing the device via the command line interface.

ICX 6430/6450 devices support two kinds of SSH client authentication: password and keyboard interactive. For password authentication, an operator attempting to establish a SSH session provides a password through the SSH client. The ICX 6430/6450 device authenticates operator with passwords stored on the device, on a TACACS+ server, or on a RADIUS server. Section 5.2 Authentication provides authentication details. The keyboard interactive (KI) authentication goes one-step ahead. It allows multiple challenges to be issued by the ICX 6430/6450 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 ICX 6430/6450 device.

SSH supports Diffie-Hellman (DH) group exchange and the client can negotiate DH Group 1 (1024 bits) to configure the modulus size on the SSH server (i.e. The ICX 6430/6450 device) for the purpose of key-exchange.

The following encryption algorithms are available for negotiation during the key exchange with a SSH client: (3des-cbc) three-key Triple-DES in CBC mode, (aes128-cbc) AES with a 128-bit key, (aes192-cbc) AES with a 192-bit key

The following MAC algorithms are available for negotiation during the key exchange with a SSH client: (hmac-sha1) HMAC-SHA1 (digest length = key length = 20 bytes)

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

4.1.2 HTTPS

This service provides a graphical user interface for managing an ICX 6430/6450 device over a secure communication channel. Using a web browser, an operator connects to a designated port on an ICX 6430/6450 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, and TLS_RSA_WITH_3DES_EDE_CBC_SHA.

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

4.1.3 SNMP

The SNMP service within user role allows read-only access to the SNMP MIB within the ICX 6430/6450 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).

4.1.4 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about an ICX 6430/6450 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.

4.2 Port Configuration Administrator Role Services

4.2.1 SSH

Section 4.1.1, above, describes this service.

The port configuration administrator will have seven commands, which allows this user to run show commands, run ping or trace route. The enable command allows the user to re-authenticate as described in section 4.1.1. Within the configuration mode, this role provides access to all the port configuration commands, e.g. all sub-commands within “interface eth 1/1” command. This operator can transfer and store firmware images and configuration files between the network and the system, and review the configuration

4.2.2 HTTPS

Section 4.1.2, above, describes this service.

Like User role, this user will get to view all the web pages. In addition, this operator will be allowed to modify any configuration that is related to an interface. For example, the Configuration->Port page will allow this operator to make changes to individual port properties within the page.

4.2.3 SNMP

Section 4.1.3, above, describes this service.

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

4.2.4 Console

Section 4.1.4, 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. EXEC commands. The list of commands available are same as those mentioned in the SSH service.

4.3 Crypto Officer Role Services

4.3.1 SSH

In addition to the two methods of authentication, password and keyboard interactive, described in section 4.1.1, SSH service in this role supports RSA or DSA public key authentication, in which the device stores a collection of client public keys. Only clients with a private key that corresponds to one of the stored public keys can gain access to the device using SSH. After a client’s public key is found to match one of the stored public keys, the device gives the Crypto Officer access to the entire module.

The Crypto Officer can perform configuration changes to the module. This role has full read and write access to The ICX 6430/6450 device.

When firmware download is desired, the Crypto Officer shall download firmware download in the primary image and secondary image.

4.3.2 SCP

This is a secure copy service. 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 MAC algorithm 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 ICX 6430/6450 devices is to copy user digital certificates and host public-private key pairs to the device in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

4.3.3 HTTPS

Section 4.1.2, above, describes this service.

In addition to Port Configuration Administrator-role capabilities, the crypto-officer has complete access to all the web pages and is allowed to make configuration updates through the web pages that support configuration changes.

4.3.4 SNMP

Section 4.1.3, above, describes this service.

The SNMP service within crypto-officer role allows read access to the SNMP MIB within The ICX 6430/6450 device, using SNMPv1, v2c or v3 versions. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. Each of the implemented SNMP v1, V2c and V3 are considered as plaintext from the perspective of FIPS 140-2 within the context of this validation; no security claim regarding SNMP is made herein. 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).

4.3.5 Console

Logging on through the CLI service is described in Section 4.1.4 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within The ICX 6430/6450 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 creates a pair of DSA host keys, to configure the authentication scheme for SSH access; afterwards the operator may securely import additional pairs of RSA host keys or pairs of DSA host keys as needed over a security SSH connection. 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.

NOTICE: The cryptographic module “does not” support RSA key generation in FIPS mode.

4.4 Non-FIPS Mode Services

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

1. 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.
2. 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).
3. SNMP
   - Allows access to Critical Security Parameter (CSP) MIB objects
4. 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.

5 Policies

5.1 Security Rules

During power-up, the module performs the following tests:

1. Triple-DES encrypt/decrypt KAT
2. AES encrypt/decrypt KAT
3. SHA-1 KAT

4. SHA-256 KAT
5. SHA-512 KAT
6. HMAC-SHA1 KAT
7. HMAC-SHA256 KAT
8. HMAC-SHA512 KAT
9. DRBG KAT
10. DSA sign/verify KAT
11. RSA sign/verify KAT
12. Firmware integrity test (DSA signature verification)

The module also supports the following conditional tests:

1. Continuous RNG test for DRBG
2. Continuous RNG test for Hardware RNG
3. Pair-wise consistency tests on generation of DSA and RSA keys
4. Firmware load test (DSA signature verification)

In case of an error, the cryptographic module returns an error number and following message will be printed on console with the appropriate reason string and the module will be reset.

FIPS Fatal Cryptographic Module Failure.

When POST is successful, the following messages will be displayed on the console:

Running fips Power on Self tests and Software/Firmware Integrity Test

fips Power on Self tests and Software/Firmware Integrity tests successful

Running continuous drbg check

Running continuous drbg check successful

Running Pairwise consistency check

RSA key pair generation succeeded

Pairwise consistency check successful

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

5.1.1 Cryptographic Module Operational Rules.

In order to operate an ICX 6430/6450 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 ICX 6430/6450 series device.

ICX 6430/6450 series devices use a FIPS Approved random number generator implementing Algorithm Hash DRBG based on hash functions.

ICX 6430/6450 devices ensure 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.

ICX 6430/6450 series devices use FIPS Approved key generation methods:

- DSA public and private keys in accordance with [FIPS 186-2+]
- RSA public and private keys in accordance with [RSA PKCS #1]

ICX 6430/6450 series devices test prime numbers generated for both DSA and RSA keys using Miller-Rabin test. See [RSA PKCS #1] Appendix 2.1 A Probabilistic Primality Test.

ICX 6430/6450 series devices use non-FIPS Approved key establishment techniques allowed for use in FIPS mode:

- Diffie-Hellman
- RSA Key Wrapping

ICX 6430/6450 series devices restrict key entry and key generation to authenticated roles.

ICX 6430/6450 series devices do not display plaintext secret or private keys. The device displays "…" in place of plaintext keys.

ICX 6430/6450 series devices use automated methods to realize session keys for SSHv2 and HTTPS.

ICX 6430/6450 series only perform "get" operations when using SNMP.

5.2 Authentication

ICX 6430/6450 devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS+, RADIUS and local configuration database. Moreover, ICX 6430/6450 devices support 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 (Console, SSH, Web, SNMP) and the order in which the device tries one or more of the following authentication methods:

a. Line password authentication,

b. Enable password authentication,

c. Local user authentication,

d. RADIUS authentication with exec authorization and command authorization, and

e. 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.

ICX 6430/6450 devices allow multiple concurrent operators through SSH and the console, only limited by the system resources.

5.2.1 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. Please note that when operating in FIPS mode, Telnet is disabled and Line Authentication is not available.

5.2.2 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.

5.2.3 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 ICX 6430/6450 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).

5.2.4 RADIUS Authentication Method

The RADIUS method uses one or more RADIUS servers to verify user names and passwords. The ICX 6430/6450 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 ICX 6430/6450 device will send the user name and password information to the next configured RADIUS server.

ICX 6430/6450 series devices support additional command authorization with RADIUS authentication. The following events occur when RADIUS command authorization takes place.

a. A user previously authenticated by a RADIUS server enters a command on The ICX 6430/6450 device.

b. The ICX 6430/6450 device looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.

c. If the command belongs to a privilege level that requires authorization, The ICX 6430/6450 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 ICX 6430/6450 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 ICX 6430/6450 device.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings.

5.2.5 TACACS+ Authentication Method

The TACACS+ method uses one or more TACACS+ servers to verify user names and passwords. For TACACS+ authentication, The ICX 6430/6450 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+ authentication, a Crypto Officer must configure TACACS+ server settings along with authentication and authorization settings.

5.2.6 Strength of Authentication

ICX 6430/6450 modules support minimum 7 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (18) in passwords. Therefore the probability of a random attempted is 1/80^7 which is less than 1/1,000,000.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one minute period is 60/80^7 which is less than 1/100,000.

5.3 Access Control Policy and Critical Security Parameter (CSP)

Table 11 Access Control Policy and Critical Security Parameter (CSP) summarizes the access operators in each role have to critical security parameters. 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 without direct access (for example encrypt with an encryption key), and
- d – operator can delete the value of the item (zeroize).

Table 11 Access Control Policy and Critical Security Parameter (CSP)

	User				Port Administrator			Crypto Officer				
Service / CSP	SSH	HTTPS	SNMP	Console	SSH	HTTPS	Console	SSH	SCP	HTTPS	SNMP	Console
SSH host RSA or DSA Private Key	x				x			xwd	x			xwd
SSH host RSA or DSA Public Key	x				x			xrwd	x			xrwd
SSH client RSA or DSA Public Key	x				x			xrwd	xrwd			xrwd
SSH KDF Internal State	x				x			x	x			
SSH DH Shared Secret Key	x				x			x	x			
TLS master secret		x				x				x		
TLS PRF Internal State		x				x				x		
SSH DH Peer Public Key	x				x							
TLS Peer Public Key		x				x				x		
SSH/SCP Session Keys and SSH/SCP Authentication Keys	x				x			x	x			
TLS host RSA Private Key		x				x		rwd	rw	x		rwd
TLS host Public Key		x				x		rwd	rw	x		rwd
TLS Pre-Master Secret		x				x		xd		x		xd
TLS Session Keys and TLS Authentication Keys		x				x		xd		x		xd
SSH DH Private Key	x				x			x	x			
SSH DH Public Key	x				x			x	x			
User Password	x	x		x	x			xrwd	xrwd	rwd		xrwd
Port Administrator Password	x				x	x		xrwd	xrwd	rwd		xrwd
Crypto Officer Password	x				x			xrwd	xrwd	xrwd		xrwd
RADIUS Secret	x	x		x	x	x		xrwd	xrwd	xrwd		xrwd
TACACS+ Secret	x	x		x	x	x		xrwd	xrwd	xrwd		xrwd
Firmware Integrity / Firmware Load DSA Public Key								x		x		x
DRBG Value V	x	x			x	x		xd	x	x		xd
DRBG Constant C	x	x			x	x		xd	x	x		xd
Hash DRBG Entropy	x	x			x	x		x	x	x		

5.4 Physical Security

ICX 6430/6450 devices require the Crypto Officer to install tamper evident seals in order to meet FIPS 140-2 Level 2 Physical Security requirements. Tamper evident seals are available for order from Brocade under FIPS Kit (Part Number: Brocade XBR-000195). The Crypto Officer shall follow the Brocade FIPS Security Seal application procedures prior to operating the module in FIPS mode. The FIPS seal application procedure is available in Appendix A of this document.

The Crypto 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 Crypto Officer shall maintain a serial number inventory of all used and unused tamper evident seals. The Crypto 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 Crypto Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

5.5 Mode Status

ICX 6430/6450 devices provide the *fips show* command to display status information about the device's FIPS mode. 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 5.5.1 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.

1. FIPS mode: Administrative Status: ON, Operational Status: OFF
    a. Some shared secrets inherited from non-fips mode may not be fips compliant and has to be zeroized. The system needs to be reloaded to operate in FIPS mode.
2. System Specific:
    a. OS monitor mode access: Disabled
3. Management Protocol Specific:
    a. Telnet server: Disabled
    b. TFTP Client: Disabled
    c. HTTPS SSL 3.0: Disabled
    d. SNMP Access to security objects: Disabled
4. Critical Security Parameter Updates across FIPS Boundary:
    a. Protocol shared secret and host passwords: Clear
    b. SSH DSA/RSA Host Keys: Clear
    c. HTTPS RSA Host Keys and Signature: Clear

The following example shows the output of the fips show command after the device reloads successfully in the default strict FIPS 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.

1. FIPS mode: Administrative Status: ON, Operational Status: ON

2. System Specific:
    a. OS monitor mode access: Disabled
3. Management Protocol Specific:
    a. Telnet server: Disabled
    b. TFTP Client: Disabled
    c. HTTPS SSL 3.0: Disabled
    d. SNMP Access to security objects: Disabled
4. Critical Security Parameter Updates across FIPS Boundary:
    a. Protocol shared secret and host passwords: Clear
    b. SSH DSA Host Keys: Clear
    c. HTTPS RSA Host Keys and Signature: Clear

5.5.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that put an ICX 6430/6450 device in FIPS Approved mode. The first action is to apply tamper evident seals to the chassis at the locations specified in the Appendix A of this document.

FIPS Approved mode disables the following:

- Telnet access including the *telnet server* command
- AAA authentication for the console including the *enable aaa console* command
- Command *ip ssh scp disable*
- TFTP access
- SNMP access to CSP MIB objects
- Access to all commands within the monitor mode
- HTTP access including the web-management http command
- Port 280
- HTTPS SSL 3.0 access
- Command web-management allow-no-password

Entering FIPS Approved mode also clears:

- Protocol shared secret and host passwords
- SSH DSA/RSA host keys
- HTTPS RSA host keys and certificate

FIPS Approved mode enables:

- SCP
- HTTPS TLS version 1.0 and greater

Table 12 Algorithm Certificates

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128, 192, and 256-bit keys, ECB and CBC mode	2243
Triple Data Encryption Algorithm (Triple-DES)	ECB and CBC mode	1403
Secure Hash Algorithm (SHS)	SHA-1, SHA-256, SHA-384, and SHA-512	1933
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	1373
Deterministic Random Bit Generator (DRBG)	SHA-256 Based SP 800-90 RBG	268
Digital Signature Algorithm (DSA)	1024-bit keys	696
Elliptic Curve Digital Signature Algorithm (ECDSA)	256, 384 and 512-bit keys	352
Rivest Shamir Adleman Signature Algorithm (RSA)	1024, 2048 and 4096-bit keys	1149

Please note: Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

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

1. RSA Key Wrapping (key establishment methodology provides 80 bits strength)
2. Diffie-Hellman (DH, 1024-bit keys) (key agreement, key establishment methodology provides 80 bits of encryption strength)
3. SNMPv3 (Cryptographic function does not meet FIPS requirements and is considered plaintext)
4. 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).
5. HMAC-MD5 – as used in RADIUS protocol (MD5 not exposed to the operator)
6. SSHv2 Key Derivation Function (KDF).

5.5.1.1 Invoke FIPS Approved Mode for Brocade ICX 6430 and ICX 6450 Devices

To invoke the FIPS Approved mode of operation, perform the following steps:

1) Assume Crypto Officer role
2) Enter command: *fips enable*

   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.
3) Enter command: *fips zeroize all*

   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.
4) Generate a pair of DSA host keys, to configure authentication scheme for SSH access; afterwards the operator may securely import additional pairs of RSA host keys of pairs of DSA host keys as needed over a secure SSH connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secure SSH connection), and enable the HTTPS server. NOTICE: The cryptographic module “does not” support RSA key generation in FIPS mode.
5) Enter command *no web-management hp-top-tools* in order to turn off access by HP ProCurve Manager via port 280
6) Save the running configuration: *write memory*

7) The device saves the running configuration as the startup configuration
8) Reload the device

   The device resets and begins operation in FIPS Approved mode.
9) Enter command: *fips show*

   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 Section 6.

5.5.1.2 Negating FIPS Approved Mode for Brocade ICX 6430 and ICX 6450 Devices

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

Brocade(config)# no fips enable

After you enter the command, a warning displays that FIPS mode will be disabled.

This command performs the following policy-related operations:

- Enables TFTP access.
- Re-enables SNMP access to Critical Security Parameter (CSP) MIB objects.
- Re-enables SNMPv3 encryption protocol DES for future SNMPv3 user configuration.
- Re-enables access to monitor mode.
- Zeroizes shared secrets, SSH and HTTPS host keys, and the HTTPS certificate based on the configured FIPS policy.

This command also performs the non-policy-related operation of re-enabling the RC4 cipher for the HTTPS server. Changes to the running configuration are not saved to the startup configuration; therefore, when the device reloads it returns to FIPS mode. Use the write memory command to save the running configuration.

6 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
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

Term/Acronym	Description
NI	NetIron
OC	Optical Carrier
POE	Power over Ethernet
POE+	High Power over Ethernet
PRF	Pseudo-random function
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS+	Terminal Access Control Access-Control System
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

7 References

[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 (Part Number: Brocade XBR-000195) contains the following items:

- Tamper Evident Security Seals
  - Count 120
  - Checkerboard destruct pattern with ultraviolet visible “Secure” image

Use 99% isopropyl alcohol 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.

The Cryptographic Officer is responsible for securing and having control of any unused seals at all times.

ICX 6430-24 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6430-24 device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel. See Figure 4 for correct seal orientation and positioning.
- **Rear**: Affix *3* seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 5 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 21.

Figure 5 Top view of a Brocade ICX 6430-24 device with security seals

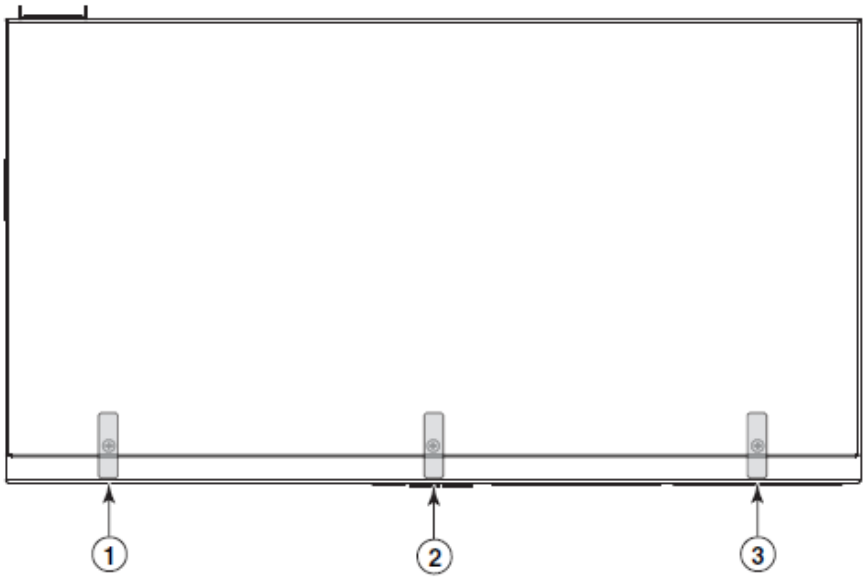
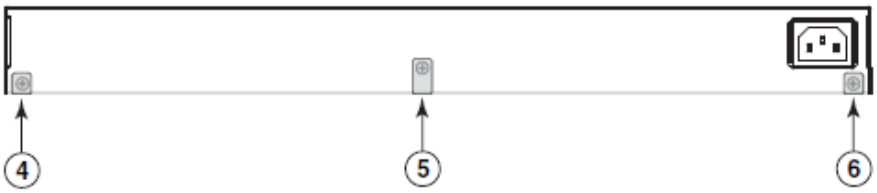


Figure 6 Rear view of a Brocade ICX 6430-24 device with security seals



ICX 6430-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6430-24P device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel as shown. See Figure 7 for correct seal orientation and portioning.
- **Rear**: Affix 3 seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 8 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 21.

Figure 7 Top view of a Brocade ICX 6430-24P device with security seals

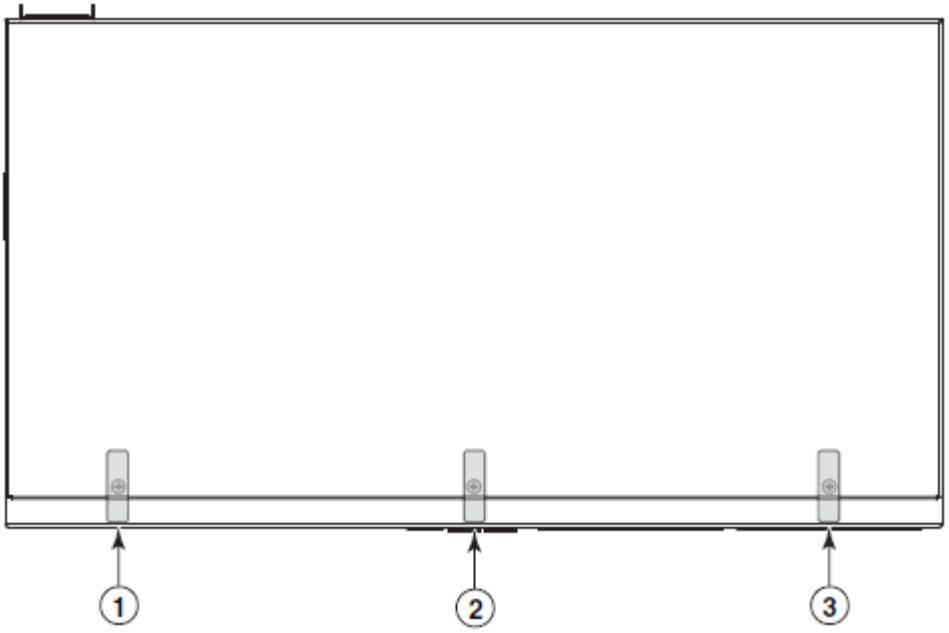
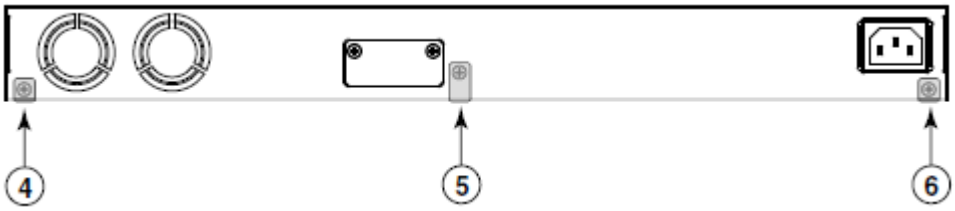


Figure 8 Rear view of a Brocade ICX 6430-24P device with security seals



ICX 6430-48 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6430-48 device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel. See Figure 9 for correct seal orientation and positioning.
- **Rear**: Affix *3* seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 10 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 22 and 23. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 9 Top view of a Brocade ICX 6430-48 device with security seals

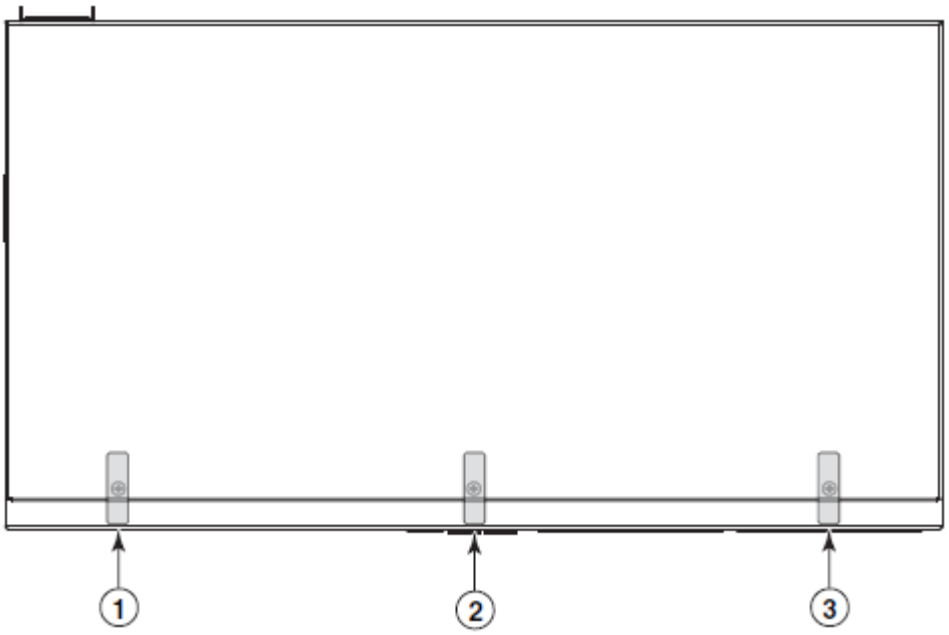
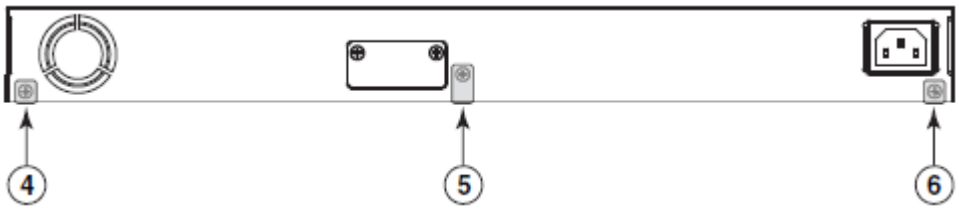


Figure 10 Rear view of a Brocade ICX 6430-48 device with security seals



ICX 6430-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6430-48P device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel as shown. See Figure 11 for correct seal orientation and portioning.
- **Rear**: Affix *3* seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 12 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 22 and 23. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 11 Top view of a Brocade ICX 6430-48P device with security seals

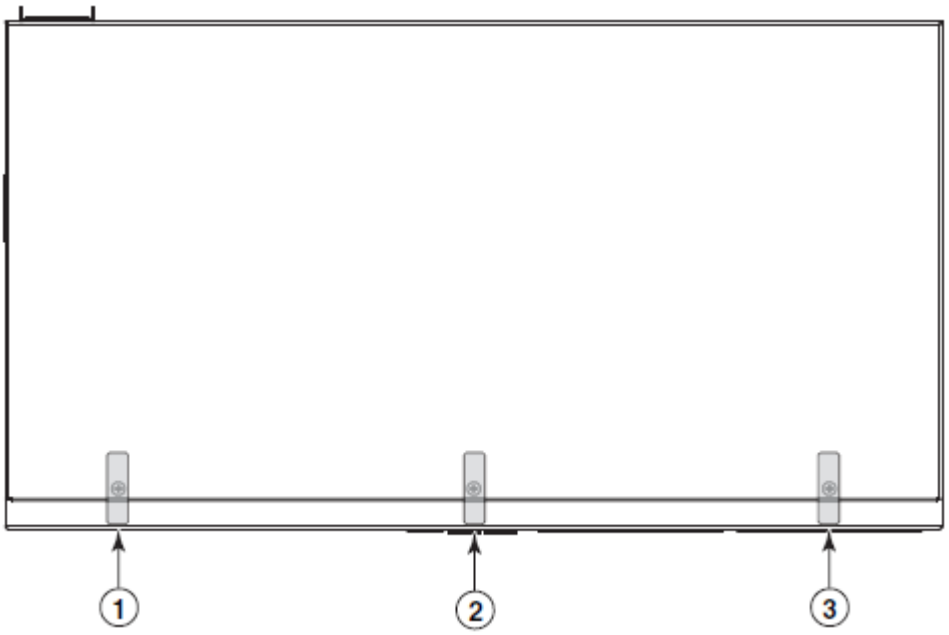
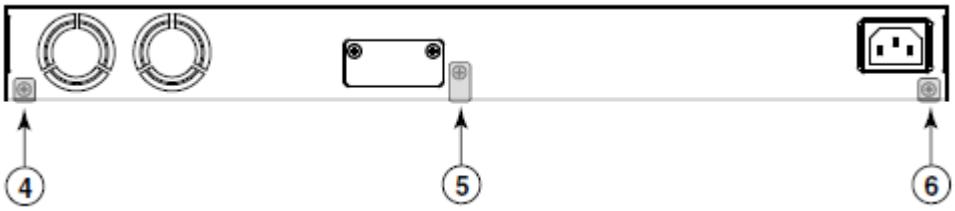


Figure 12 Rear view of a Brocade ICX 6430-48P device with security seals



ICX 6450-24 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450-24 device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel. See Figure 13 for correct seal orientation and positioning.
- **Rear**: Affix *3* seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 14 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 21.

Figure 13 Top view of a Brocade ICX 6450-24 device with security seals

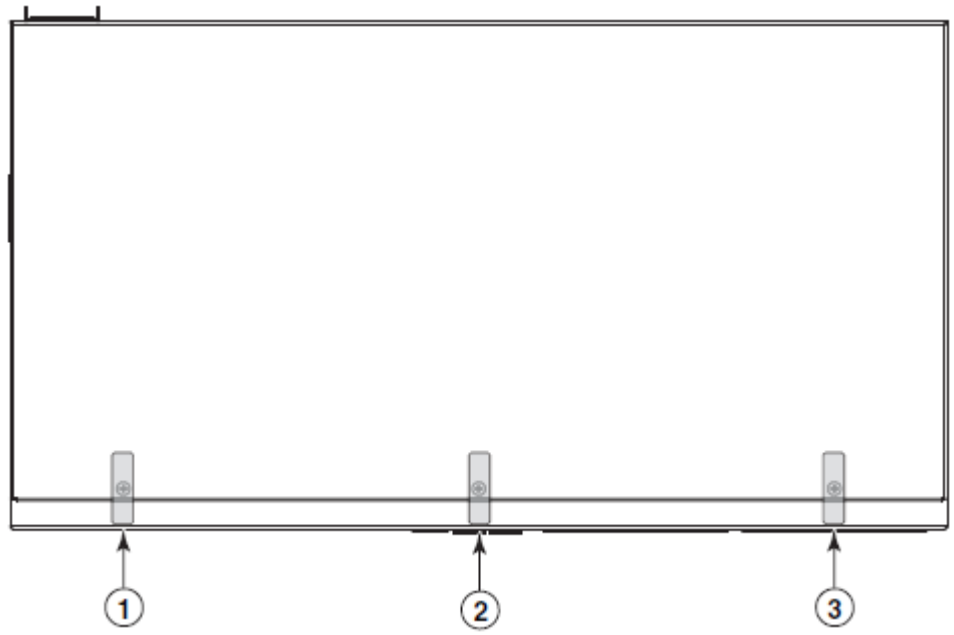
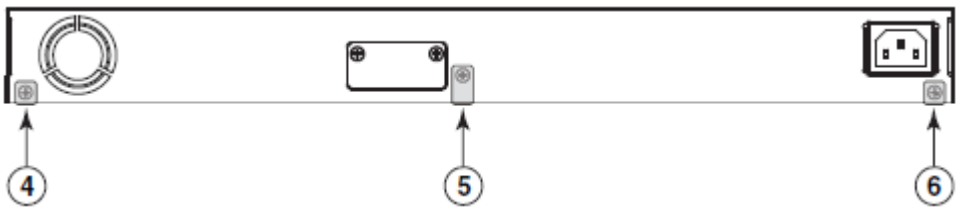


Figure 14 Rear view of a Brocade ICX 6450-24 device with security seals



ICX 6450-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 24P device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel as shown. See Figure 15 for correct seal orientation and portioning.
- **Rear**: Affix *3* seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 16 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 21.

Figure 15 Top view of a Brocade ICX 6450-24P device with security seals

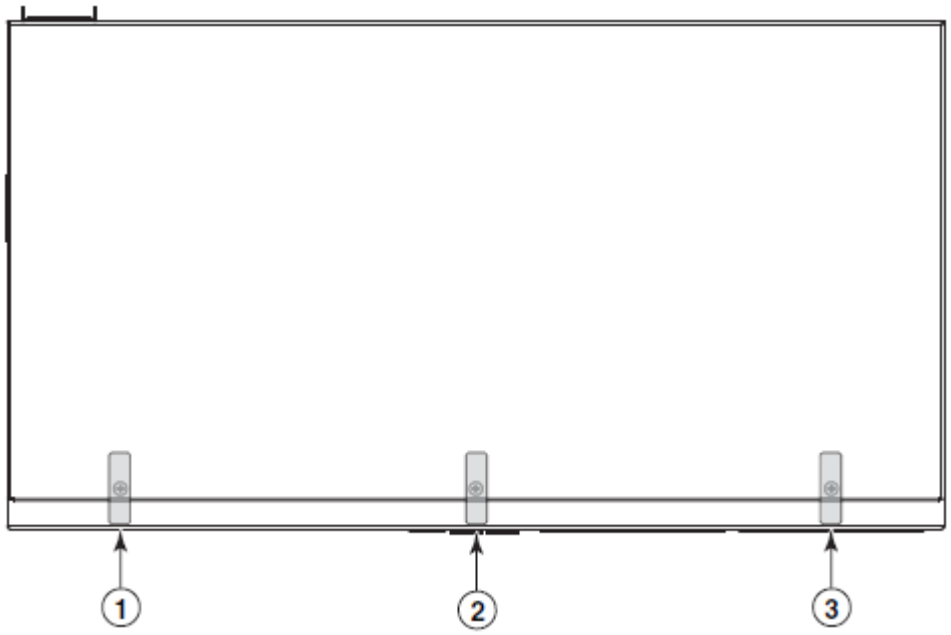
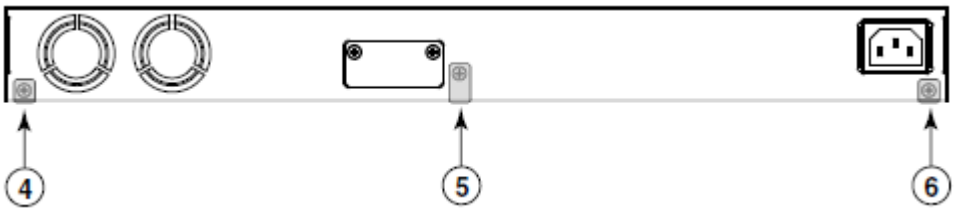


Figure 16 Rear view of a Brocade ICX 6450-24P device with security seals



ICX 6450-48 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 48 device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel. See Figure 17 for correct seal orientation and positioning.
- **Rear**: Affix *3* seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 18 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 22 and 23. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 17 Top view of a Brocade ICX 6450-48 device with security seals

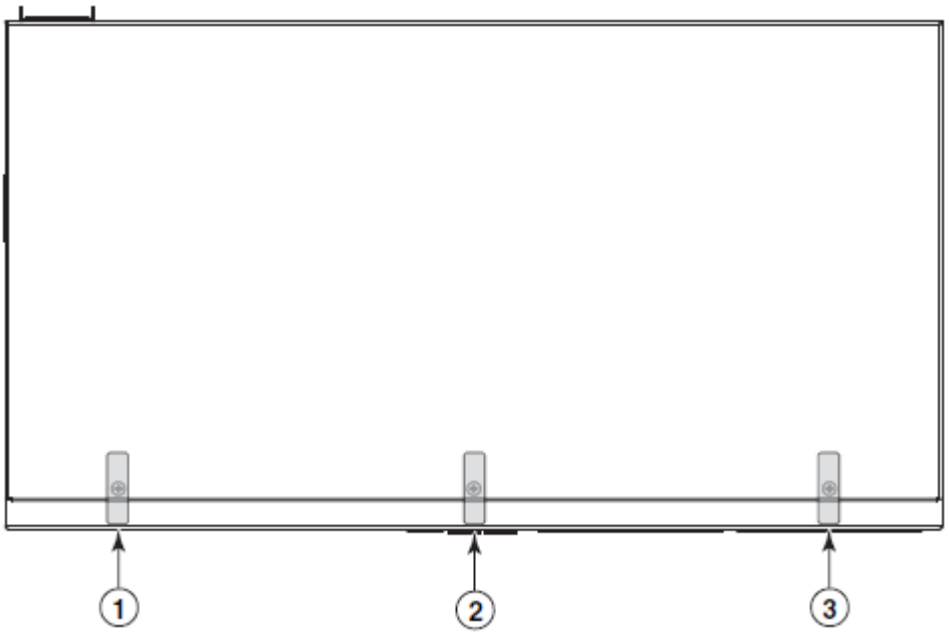
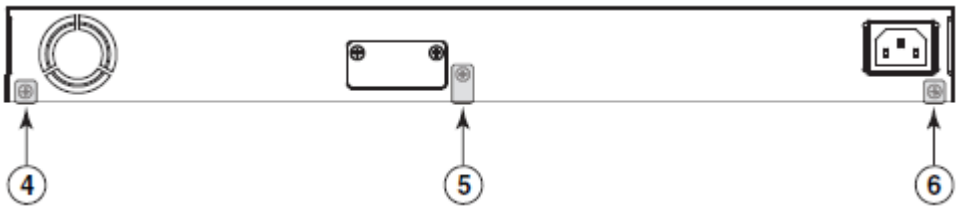


Figure 18 Rear view of a Brocade ICX 6450-48 device with security seals



ICX 6450-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450 - 48P device. Each device requires the placement of seven seals:

- **Top**: Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal on the metal cover and other part is affixed over the top of the front panel as shown. See Figure 19 for correct seal orientation and portioning.
- **Rear**: Affix *3* seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part the seal is affixed to the chassis bottom and part is affixed to the rear cover as shown. Refer to Figure 20 for correct seal orientation and positioning.
- **Console Port**: Affix 1 seal over the console port, as shown in Figure 22 and 23. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure 19 Top view of a Brocade ICX 6450-48P device with security seals

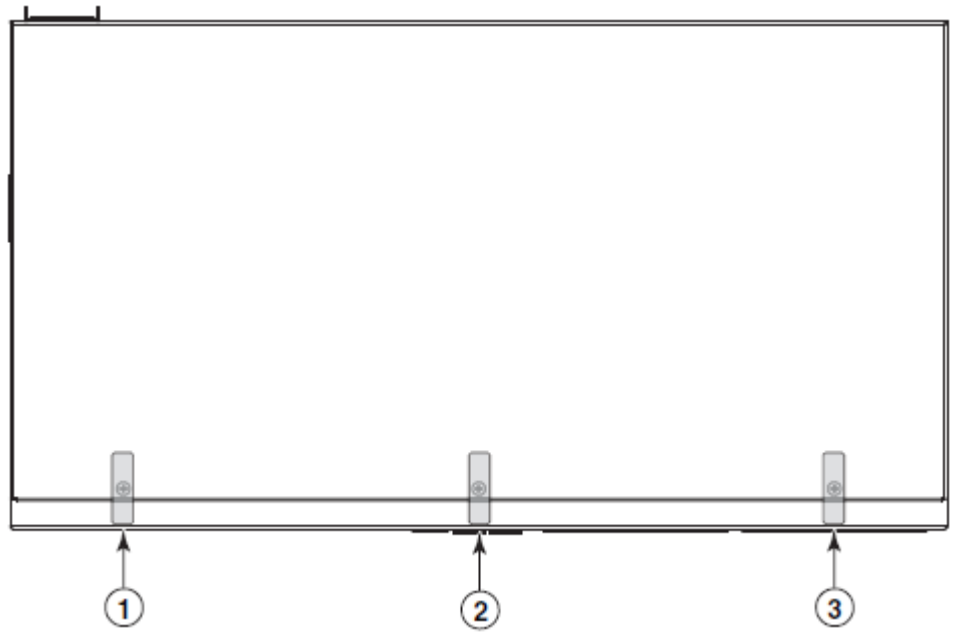


Figure 20 Rear view of a Brocade ICX 6450-48P device with security seals

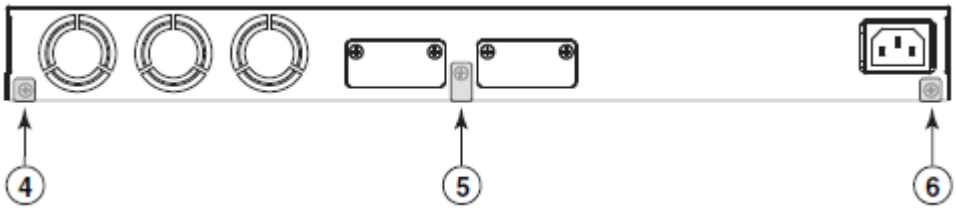


Figure 21 Security Seal over the console port on the Brocade ICX 6430-24, ICX 6430-24P, ICX 6450-24 and ICX 6450-24P devices

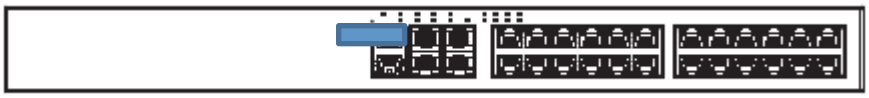


Figure 22 Security Seal over the console port on the Brocade ICX 6430-48, ICX 6430-48P, ICX 6450-48 and ICX 6450-48P devices

Figure 23 Side View of Security Seal over the console port on the Brocade ICX 6430-48, ICX 6430-48P, ICX 6450-48 and ICX 6450-48P devices