Brocade ICX 6610 Series
Stackable Switch with FastIron 7.3.00c Firmware

FIPS 140-2 Non-Proprietary Security Policy
Level 2 with Design Assurance Level 3 Validation

Document Version 0.8
June 25, 2013

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. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

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

The Brocade ICX 6610 series stackable switches are part of Brocade's ICX 6610 product family. They are designed for medium to large enterprise backbones. The ICX 6610 series is an access layer Gigabit Ethernet switch designed from the ground up for the enterprise data center environment.

2 Overview

The FIPS140-2 validation includes the 10 (ten) hardware devices presented in Table 2 running the firmware version presented in Table 1, referred collectively for the remainder of this document as ICX 6610 device (cryptographic module, or simply the module). Each ICX 6610 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. Five (5) models are available in the ICX 6610 series. The installed fans either use a push or pull configuration to move the air between the back and front of the device. Each model is orderable with either fan trays or power supply side intake (-I) or power supply side exhaust (-E) airflow, therefore two SKUs per module is listed in Table 2. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. The cryptographic boundary for each ICX 6610 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 6610 series (listed in Table 2 ICX 6610 Switch Family Part Numbers) run the same firmware version that includes the cryptographic functionality described on page 9. The "–E" and "–I" designations in Table 2 define the airflow direction as either intake or exhaust. The "-24" and "-48" designations in Table 2 define the port count, and the designator "P" following the port count indicate PoE+ ports;; the designator "F" indicate Small Form-Factor Pluggable (SFP) ports, per table Table 3 ICX 6610 Series Physical Ports. Otherwise, devices with similar SKUs are identical.

Table 1 Firmware Version

Firmware Version
FI 7.3.00c

2.2 ICX6610 Series

Table 2 ICX 6610 Switch Family Part Numbers

	SKU	MFG Part Number	Brief Description
#1	ICX 6610-24F-I	80-1005350-03	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side intake airflow ("-I" in the SKU)
#2	ICX 6610-24F-E	80-1005345-03	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side exhaust airflow ("-E" in the SKU)
#3	ICX 6610-24-I	80-1005348-04	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow ("-I" in the SKU)
#4	ICX 6610-24-E	80-1005343-04	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow ("-E" in the SKU)
#5	ICX 6610-24P-I	80-1005349-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow ("-I" in the SKU)

	SKU	MFG Part Number	Brief Description
#6	ICX 6610-24P-E	80-1005344-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow ("-E" in the SKU)
#7	ICX 6610-48-I	80-1005351-04	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow ("-I" in the SKU)
#8	ICX 6610-48-E	80-1005346-04	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow ("-E" in the SKU)
#9	ICX 6610-48P-I	80-1005352-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow ("-I" in the SKU)
#10	ICX 6610-48P-E	80-1005347-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow ("-E" in the SKU)
#1 through #10 above must be configured with FIPS Kit	Brocade XBR-000195		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 6610-24 and ICX 6610-24P cryptographic modules (#3, #4, #5 and #6 in Table 2 ICX 6610 Switch Family Part Numbers).

Figure 1 ICX 6610-24 and ICX 6610-24P cryptographic modules

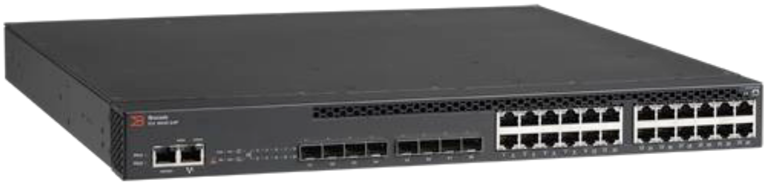

Figure 2 illustrates the ICX 6610-48 and ICX 6610-48P cryptographic modules (#7, #8, #9 and #10 in Table 2 ICX 6610 Switch Family Part Numbers).

Figure 2 ICX 6610-48 and ICX 6610-48P cryptographic modules

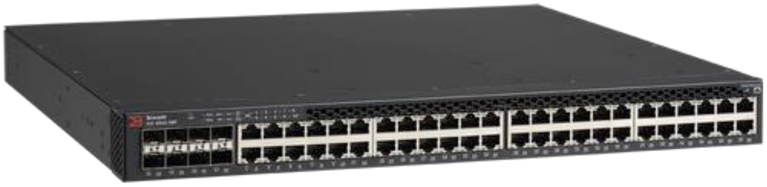

Figure 3 illustrates the ICX 6610-24F cryptographic module (#1 and #2 in Table 2 ICX 6610 Switch Family Part Numbers).

Figure 3 ICX 6610-24F cryptographic module

2.3 Ports and Interfaces

Each ICX 6610 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.

Though not part of this validation, the ICX 6610 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 network ports provided by each ICX 6610 model. Table 4 shows the correspondence between the physical interfaces of ICX 6610 devices and the logical interfaces defined in FIPS 140-2.

Table 3 ICX 6610 Series Physical Ports

ICX6610 series	Dual-mode 1 GbE/10 GbE SFP/SFP+ ports	10/100/1000 Mbps RJ-45 ports	1 GbE SFP ports	40 Gbps high-performance QSFP stacking ports[1]	AC inlet[2]	Reset	Out of band management ports	LEDs													
								Ethernet		PoE+			System Status								
								Speed	Status	Speed	Status	SFP/SFP+	PSU 1	PSU 2	DIAG	XL 1	XL	MS	XL2-XL5	XL7-XL10	Stack ID[3]
ICX 6610-24F-I, ICX 6610-24F-E	8	N/A	24	4	2	1	2	NA	NA	NA	NA	32	1	1	1	1	1	1	1	1	10
ICX 6610-24-I, ICX 6610-24-E	8	24	NA	4	2	1	2	24	24	NA	NA	8	1	1	1	1	1	1	1	1	10
ICX 6610-24P-I, ICX 6610-24P-E	8	24	NA	4	2	1	2	NA	NA	24	24	8	1	1	1	1	1	1	1	1	10
ICX 6610-48-I, ICX 6610-48-E	8	48	NA	4	2	1	2	48	48	NA	NA	8	1	1	1	1	1	1	1	1	10
ICX 6610-48P-I, ICX 6610-48P-E	8	48	NA	4	2	1	2	NA	NA	48	48	8	1	1	1	1	1	1	1	1	10

[1] Used exclusively for stacking. Stacking functionality is explicitly disabled in FIPS mode.
[2] One AC inlet per installed power supply. Shown value represents the maximum available
[3] nominal – Stack ID1, Stack ID2, …

Table 4 Port mapping to logical interface

Physical Port	Logical Interface
Dual-mode 1 GbE/10 GbE SFP/SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
1 GbE SFP ports	Data input/Data output, Status output
40 Gbps high-performance QSFP stacking ports	Data input/Data output, Status output
AC inlet	Power
Out of band management ports[i]	Control input, Status output
Reset	Control input
LED	Status output

2.4

2.4 Modes of Operation

The ICX 6610 cryptographic 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 5 ICX 6610 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 6610 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 6610 modules do not have a maintenance interface or maintenance role.

Section 5.2 Authentication described 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 6610 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 6 FIPS Approved Cryptographic Functions" summarizes the available FIPS-Approved cryptographic functions. "Table 7 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 6 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

Table 7 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	Message-Digest algorithm (not exposed to the operator: internal to TLS v1.0, TACACS+ and RADIUS)
KDF	SSHv2 Key Derivation Function
HWRNG	Generation of seeds for DRBG

Table 8 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_SHA_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-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

4.1 User Role Services

4.1.1 SSH

This service provides a secure session between an ICX 6610 device and a SSH client using SSHv2 protocol. The ICX 6610 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 6610 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 6610 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 6610 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 6610 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 6610 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 6610 device over a secure communication channel. Using a web browser, an operator connects to a designated port on an ICX 6610 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 will not be allowed to make any modifications. If the user presses the ‘Modify’ button within any page, he will be challenged to reenter his credentials. The challenge dialog box will not be closed without proper access credentials of the crypto-officer. 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 6610 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 6610 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

This service is described in Section 4.1.1 above.

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

This service is described in Section 4.1.2 above.

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

The SNMP service is not available for a port configuration administrator role service.

4.2.4 Console

This service is described in Section 4.1.4 above. 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 will give 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 6610 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 6610 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

This service is described in section 4.2.2 HTTPS.

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

The SNMP service within crypto-officer role allows read access to the SNMP MIB within the ICX 6610 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 6610 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 secured 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 secured SSH connection), and enable the HTTPS server.

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

5 Policies

5.1 Security Rules

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

1. TripleDES 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. CRNGT for DRBG
2. CRNGT for Hardware RNG
3. Pair-wise consistency tests on generation of DSA and RSA keys

   NOTICE: The module supports a pairwise consistency test for RSA key generation, however RSA key generation “is not” supported in FIPS mode.
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. In order to operate an ICX 6610 series device securely, an operator should be aware of the following rules for FIPS Approved mode of operation.

External communication channels / ports shall not be available before initialization of an ICX 6610 series device.

ICX 6610 series devices shall use a FIPS Approved random number generator implementing Algorithm Hash DRBG based on hash functions.

ICX 6610 devices shall ensure the random number seed and seed key input do not have same value. The devices shall generate seed keys and shall not accept a seed key entered manually.

ICX 6610 series devices shall 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]
    - NOTICE: The cryptographic module "does not" support RSA key generation in FIPS mode.

ICX 6610 series devices shall 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.

- NOTICE: The cryptographic module "does not" support RSA key generation in FIPS mode.

ICX 6610 series devices shall use Approved key establishment techniques:

- Diffie-Hellman
- RSA Key Wrapping

ICX 6610 series devices shall restrict key entry and key generation to authenticated roles.

ICX 6610 series devices shall not display plaintext secret or private keys. The device shall display "..." in place of plaintext keys.

ICX 6610 series devices shall use automated methods to realize session keys for SSHv2 and HTTPS.

ICX 6610 series shall only perform "get" operations using SNMP.

5.2 Authentication

ICX 6610 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 6610 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 (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 6610 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 6610 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 6610 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 6610 device will send the user name and password information to the next configured RADIUS server.

ICX 6610 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 6610 device.

b. The ICX 6610 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 6610 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 6610 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 6610 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 6610 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 6610 devices minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 7 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (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.

The probability of a successful random guess of a RADIUS or TACACS+ password during a one-minute period is less than 3 in 1,000,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

5.3 Table 9 Access Control Policy and CSP access 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 9 Access Control Policy and CSP access

	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 DH Private Exponent	x				x			x	x			
SSH DH Public Key	x				x			x	x			
SSH session keyset	x				x			x	x			
TLS host RSA private key		x				x		rwd	rw	x		rwd
TLS host RSA digital certificate		x				x		rwd	rw	x		rwd
TLS pre-master secret		x				x		xd		x		xd
TLS session keyset		x				x		xd		x		xd
DRBG Value V	x	x			x	x		xd	x	x		xd
DRBG Constant C	x	x			x	x		xd	x	x		xd
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								xrwd		xrwd		xwd

5.4 Physical Security

ICX 6610 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 defined in Appendix A of this document prior to operating the module in FIPS mode.

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.

Please refer to Appendix A of this Security Policy document for specific tamper evident seal application instructions.

5.5 Mode Status

ICX 6610 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
    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 6610 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 10 Algorithm Certificates

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128, 192, and 256-bit keys, ECB and CBC mode	#2150
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	#1363
Secure Hash Algorithm (SHS)	SHA-1, SHA-256, SHA-384, and SHA-512	#1871
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1317
Deterministic Random Bit Generator (RBG)	SHA-256 Based SP 800-90 RBG	#239
Digital Signature Algorithm (DSA)	1024-bit keys	#668
Elliptic Curve Digital Signature Algorithm (ECDSA)	256, 384 and 512-bit keys	#324
Rivest Shamir Adleman Signature Algorithm (RSA)	1024, 2048 and 4096-bit keys	#1106

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

1. RSA (key wrapping; key establishment methodology provides 80 bits of encryption 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 – as used in the TLS v1.0 pseudo-random function (PRF) in FIPS mode (MD5 not exposed to the operator) ; as used in TACACS+ packets for message integrity verification (MD5 not exposed to the operator).
5. HMAC-MD5 (MD5 is not exposed to the operator; only used to support legacy systems; Cryptographic function does not meet FIPS requirements and is considered plaintext)
6. SSHv2 Key Derivation Function (KDF)

5.5.1.1 Invoke FIPS Approved Mode

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 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 secured 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 secured 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.

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
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 6610-24F Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-24F device. Each device requires the placement of eighteen seals:

- Front: Affix one seal (1) over the console port on the left side of the front panel. The seal should be centered on port and adhere to the front panel above and below the port. See Figure 4 and Figure 5 for correct seal orientation and positioning.
- Top: Affix five 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 is on the metal cover and other part is affixed to the front panel as shown. See Figure 5 for correct seal orientation and positioning.
- Right and left sides: Affix two seals to each side of the device. Place the seals in a 90 degree bend, so that part the seal is affixed to the side of the device and part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 5 for correct seal orientation and positioning on the side of the device.

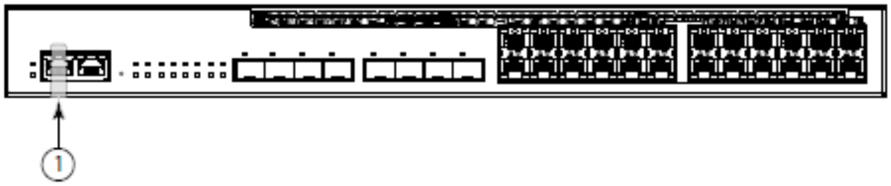

Figure 4 Front view of a Brocade ICX 6610-24F device with security seals

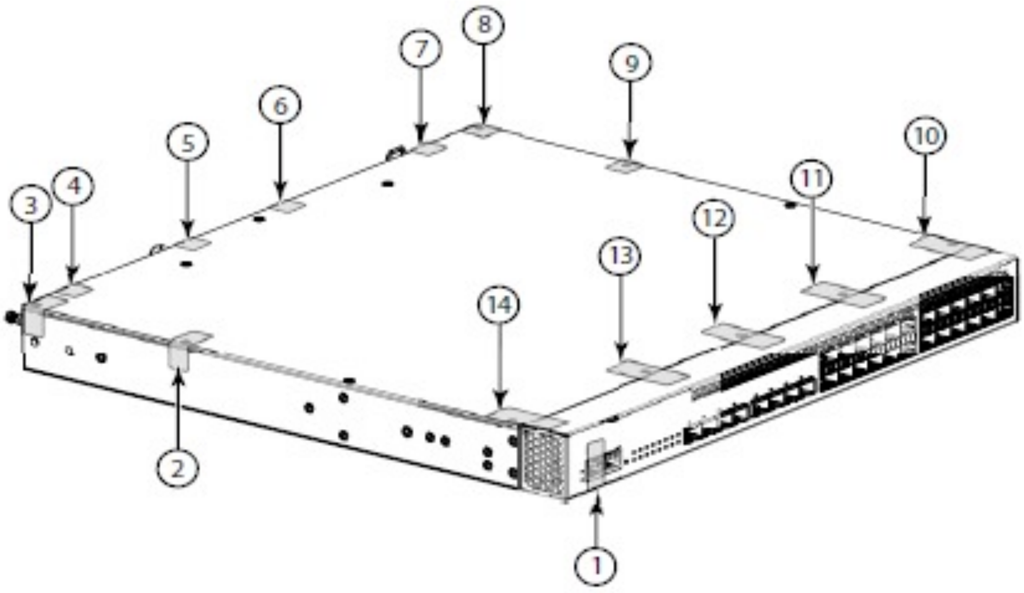

Figure 5 Top, front, and right side view of a Brocade ICX 6610-24F device with security seals

- Rear: Affix eight seals to the backside of the device. Place four seals between the top removable cover and the rear panel and 4 between the bottom of the chassis and the rear panel. Place the seals in a 90 degree bend, so that part the seal is affixed to the rear panel of the device and part is affixed to the top cover or chassis bottom. Refer to Figure 6 for correct seal orientation and positioning.
  - Note the placement of the seal (15) below the power supply handle.

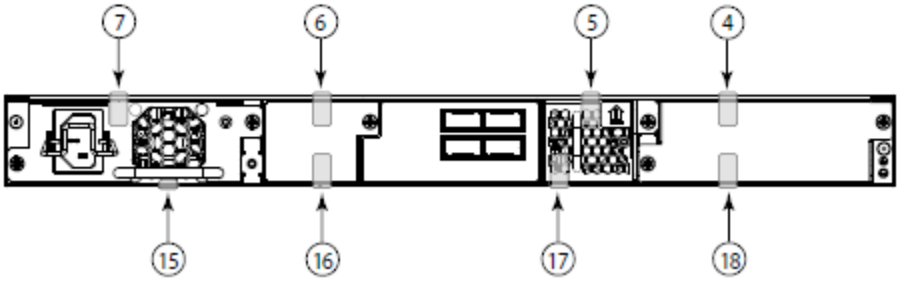

Figure 6 Rear view of a Brocade ICX 6610-24F device with security seals

ICX 6610-24 and ICX 6610-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-24 and ICX 6610-24P devices. Each device requires the placement of eighteen seals:

- Front: Affix one seal (1) over the console port on the left side of the front panel. The seal should be centered on port and adhere to the front panel above and below the port. See Figure 7 and Figure 8 for correct seal orientation and positioning.
- Top: Affix five 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 is on the metal cover and other part is affixed to the front panel as shown. See Figure 8 for correct seal orientation and positioning.
- Right and left sides: Affix two seals to each side of the device. Place the seals in a 90 degree bend, so that part the seal is affixed to the side of the device and part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 8 for correct seal orientation and positioning on the side of the device.

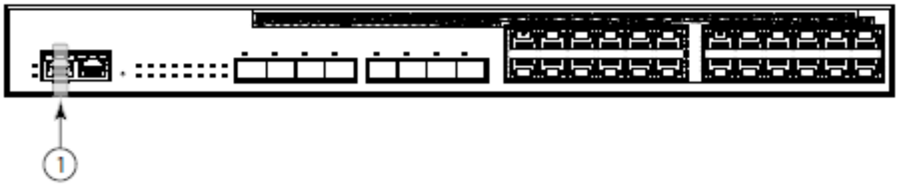

Figure 7 Front view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals

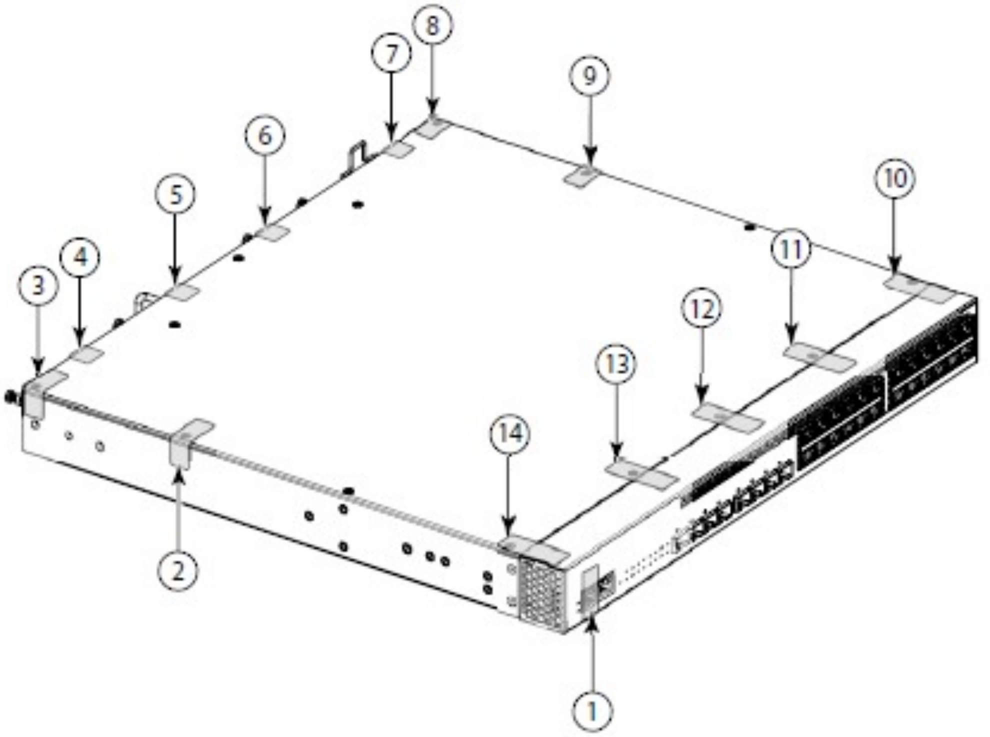

Figure 8 Front, top, and left side view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals

- Rear: Affix eight seals to the rear of the device. Place four seals between the top removable cover and the rear panel and four between the bottom of the chassis and the rear panel. Place the seals in a 90-degree bend, so that part the seal is affixed to the rear panel of the device and part is affixed to the top cover or chassis bottom as shown. Refer to Figure 9 for correct seal orientation and positioning.
  - Note the placement of the seal (15) below the power supply handle.

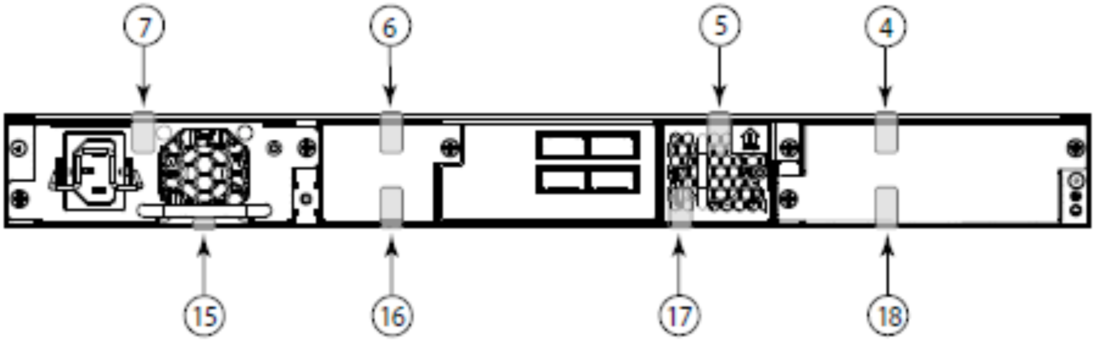

Figure 9 Rear view of Brocade ICX 6610-24 and ICX 6610-24P devices with security seals

ICX 6610-48 and ICX 6610-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6610-48 and ICX 6610-48P devices. Each device requires the placement of eighteen seals.

- Top: Affix five 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 is on the metal cover and other part is affixed to the front panel as shown. See Figure 10 for correct seal orientation and positioning.
- Right and left sides: Affix two seals to each side of the device. Place the seals in a 90-degree bend, so that part the seal is affixed to the side of the device and part is affixed to the removable top cover as shown. The orientation and placement of seals on the left side of the device mirrors the orientation and placement of seals on the right side of the device. Refer to Figure 10 for correct seal orientation and positioning on the side of the device.

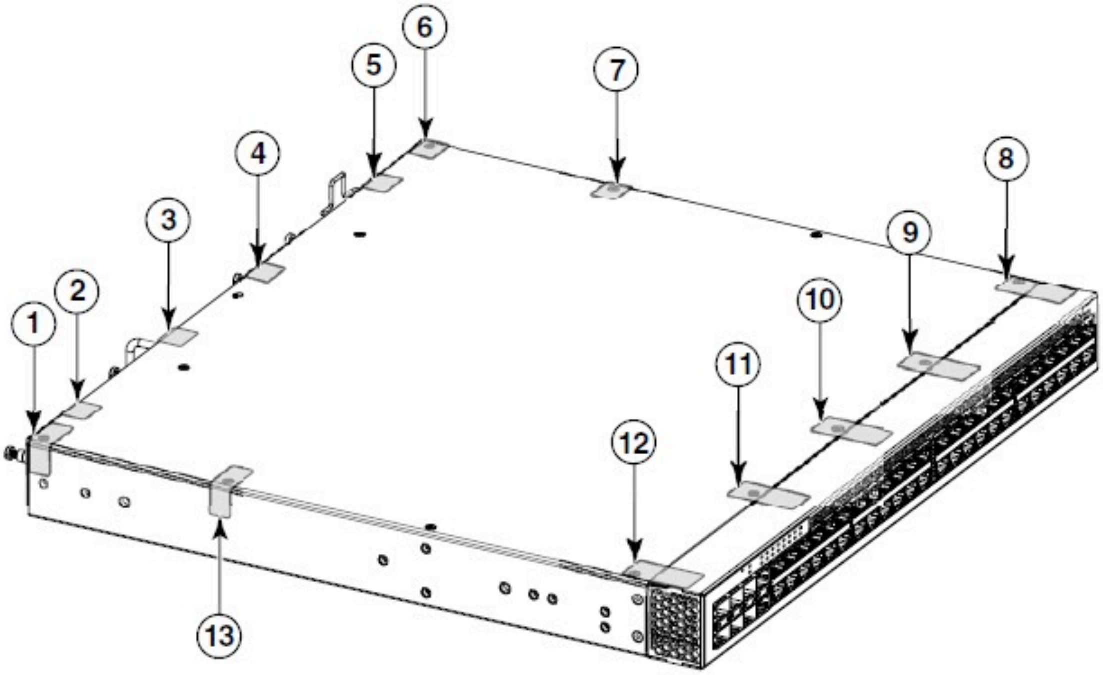

Figure 10 Front, top, and left side view of Brocade ICX 6610-48 and ICX 6610-48P devices with security seals

- Rear: Affix nine seals to the rear of the device. Place four seals between the top removable cover and the rear panel and four between the bottom of the chassis and the rear panel. Place the seals in a 90-degree bend, so that part the seal is affixed to the rear panel of the device and part is affixed to the top cover or chassis bottom. Affix one seal (16) so that it covers the console port in the center of the rear panel and is oriented vertically. The seal should be centered on port and adhere to the rear panel above and below the port. Refer to Figure 11 for correct seal orientation and positioning.
    - Note the placement of the seal (14) below the power supply handle.

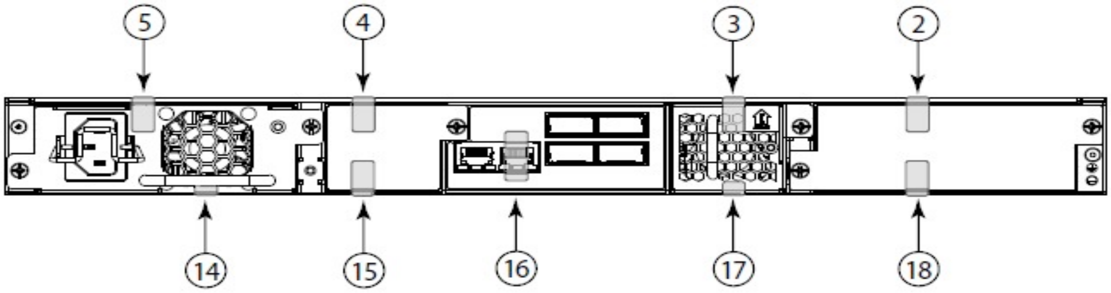

Figure 11 Rear view of Brocade ICX 6610-48 and ICX 6610-48P devices with security seals