Brocade® ICX™ 6610 and ICX 7450 Series

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

Document Version 1.1

July 11, 2016

Revision History:

Revision Date	Revision	Summary of Changes
5/9/2016	1.0	Initial Release
7/11/2016	1.1	Updates to Section 7.3, 10.3 and Appendix B

Table of Contents:

1 Introduction 10
2 Overview 10
3 FastIron Firmware 11
4 ICX 6610 Series 12
5 ICX 7450 Series 18
6 Ports and Interfaces 33
6.1 ICX 6610 Series 33
6.2 ICX 7450 Series 34
7 Modes of Operation 38
7.1 Module Validation Level 38
7.2 Roles 38
7.3 Services 39
7.4 User Role Services 43
7.4.1 SSHv2 43
7.4.2 HTTPS 44
7.4.3 SNMP 44
7.4.4 Console 44
7.4.5 NTP 44
7.5 Port Configuration Administrator Role Services 45
7.5.1 SSHv2 45
7.5.2 HTTPS 45
7.5.3 SNMP 45
7.5.4 Console 45
7.5.5 NTP 45
7.6 Crypto Officer Role Services 46
7.6.1 SSHv2 46
7.6.2 SCP 46
7.6.3 HTTPS 46
7.6.4 SNMP 46
7.6.5 Console 46
7.6.6 NTP 47
7.7 MACsec Peer Role Services 47

7.7.1 MACsec 47
8 Policies 47
8.1 Security Rules 47
8.1.1 FIPS Fatal Cryptographic Module Failure 49
8.2 Authentication 50
8.2.1 Line Password Authentication Method 51
8.2.2 Enable Password Authentication Method 51
8.2.3 Local Password Authentication Method 51
8.2.4 RADIUS Authentication Method 51
8.2.5 TACACS+ Authentication Method 52
8.2.6 Pre-shared keys Method 52
8.2.7 Strength of Authentication 52
8.2.7.1 MACsec Peer Role (only) 52
8.2.7.2 All other roles (except MACsec Peer Role) 53
8.2.8 Access Control Policy and CSP & Public Key access 54
9 Physical Security 57
10 Description of FIPS Approved Mode 58
10.1 FIPS Approved Mode 58
10.2 Displaying Mode Status 64
10.3 Invoking FIPS Approved Mode 66
11 Glossary 68
12 References 69
13 Appendix A: Tamper Evident Label application 70
13.1 ICX 6610 devices 71
13.1.1 ICX6610-24F Devices 71
13.1.2 ICX6610-24 and ICX6610-24P Devices 74
13.1.3 ICX6610-48 and ICX6610-48P Devices 77
13.2 ICX 7450 Devices 79
14 Appendix B: Critical Security Parameters 82

Table of Tables:

Table 1 - Firmware Version 11
Table 2 - ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules 12
Table 3 - ICX 7450 Switch Family Part Numbers of Validated Cryptographic Modules 18
Table 4 - Components of the ICX 7450 Series 18
Table 5 - ICX 7450 Support Matrix 20
Table 6 - ICX 6610 Series Physical Ports 33
Table 7 - ICX 6610 Port mapping to logical interface 34
Table 8 - ICX 7450 Port mapping to logical interface 34
Table 9 - Management port (10/100/1000 Mbps) status LED 35
Table 10 - 100/1000 Mbps RJ-45 port LEDs 35
Table 11 - 100/1000 Mbps RJ-45 PoE LEDs 35
Table 12 - 100/1000 Mbps SFP port LEDs 35
Table 13 - 1/10 Gbps RJ-45 port LEDs 35
Table 14 - 1/10 GbE SFP+ module port LEDs 36
Table 15 - 40 GbE mode QSFP+ module port LEDs (left-side LED) 36
Table 16 - 4x10 GbE mode QSFP+ module port LEDs 36
Table 17 ICX 7450 - PSU1 and PSU2 LEDs 36
Table 18 - ICX 7450 - DIAG LED 36
Table 19 - ICX 7450 - MS LED 37
Table 20 - ICX 7450 - MOD LED 37
Table 21 - ICX 7450 - Stack ID LEDs 37
Table 22 - ICX 7450 - Module Power LED (all media/stacking modules) 37
Table 23 - Security Requirements and Levels 38
Table 24 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode 39
Table 25 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode 40
Table 26 - FIPS non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode 42
Table 27 - Access Control Policy and CSP & Public Key access 56
Table 28 - Access Control Policy and CSP access for MACsec Peer role 56
Table 29 - Algorithm Certificates for the ICX 6610 Devices 60
Table 30 - Algorithm Certificates for the ICX 7450 Devices 62
Table 31 – RSA Algorithm Certificates usage 63

Table 32 - Glossary 68

Table of Figures:

Figure 1 - Block diagram 11
Figure 2 - Front and top side of the Brocade ICX 6610-24 13
Figure 3 - Back side of the Brocade ICX 6610-24 13
Figure 4 - Left side of the Brocade ICX 6610-24 13
Figure 5 - Right side of the Brocade ICX 6610-24 13
Figure 6 - Bottom side of the Brocade ICX 6610-24 13
Figure 7 - Front and top side of the Brocade ICX 6610-24P 14
Figure 8 - Back side of the Brocade 6610-24P 14
Figure 9 - Left side of the Brocade 6610-24P 14
Figure 10 - Right side of the Brocade 6610-24P 14
Figure 11 - Bottom side of the Brocade 6610-24P 14
Figure 12 - Front and top side of the Brocade ICX 6610-24F 15
Figure 13 - Back side of the Brocade ICX 6610-24F 15
Figure 14 - Left side of the Brocade ICX 6610-24F 15
Figure 15 - Right side of the Brocade ICX 6610-24F 15
Figure 16 - Bottom side of the Brocade ICX 6610-24F 15
Figure 17 - Front and top side of the Brocade ICX 6610-48 16
Figure 18 - Back side of the Brocade ICX 6610-48 16
Figure 19 - Left side of the Brocade ICX 6610-48 16
Figure 20 - Right side of the Brocade ICX 6610-48 16
Figure 21 - Bottom side of the Brocade ICX 6610-48 16
Figure 22 -Front and top side of the Brocade ICX 6610-48P 17
Figure 23 - Back side of the Brocade ICX 6610-48P 17
Figure 24 - Left side of the Brocade ICX 6610-48P 17
Figure 25 - Right side of the Brocade ICX 6610-48P 17
Figure 26 - Bottom side of the Brocade ICX 6610-48P 17
Figure 27 - Front/top side of the module ICX7450-24 with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ 21
Figure 28 - Back side of the module ICX7450-24 with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom] 21
Figure 29 - Left side of the module ICX7450-24 22
Figure 30 - Right side of the module ICX7450-24 22
Figure 31 - Bottom side of the module ICX7450-24 22

Figure 32 - Front/top side of the module ICX7450-24P with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ 23
Figure 33 - Back side of the module ICX7450-24P with ICX7400-4X10GC, ICX7400-1X40GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom] 24
Figure 34 - Left side of the module ICX7450-24P 24
Figure 35 - Right side of the module ICX7450-24P 25
Figure 36 - Bottom side of the module ICX7450-24P 25
Figure 37 - Front/top side of the module ICX7450-48 with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF 26
Figure 38 - Back side of the module ICX7450-48 with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom] 26
Figure 39 - Left side of the module ICX7450-48 27
Figure 40 - Right side of the module ICX7450-48 27
Figure 41 - Bottom side of the module ICX7450-48 27
Figure 42 - Front/top side of the module ICX7450-48P with ICX74004X1GF, ICX7400-4X10GC and ICX7400-4X10GF 28
Figure 43 - Back side of the module ICX7450-48P with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom] 29
Figure 44 - Left side of the module ICX7450-48P 29
Figure 45 - Right side of the module ICX7450-48P 30
Figure 46 - Bottom side of the module ICX7450-48P 30
Figure 47 - Front/top side of the module ICX7450-48F with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF 31
Figure 48 - Back side of the module ICX7450-48F with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom] 31
Figure 49 - Left side of the module ICX7450-48F 32
Figure 50 - Right side of the module ICX7450-48F 32
Figure 51 - Bottom side of ICX7450-48F 32
Figure 52 - ICX6610-24F - Front view with tamper evident label security seals 71
Figure 53 - ICX6610-24F - Top, front and left side view with tamper evident label security seals 72
Figure 54 - ICX6610-24F - Rear view with tamper evident label security seals 73
Figure 55 - ICX6610-24 and ICX6610-24P - Front view with tamper evident label security seals 74
Figure 56 - ICX6610-24 and ICX6610-24P - Front, top and left side view with tamper evident label security seals 75
Figure 57 - ICX6610-24 and ICX6610-24P - Rear view with tamper evident label security seals 76

Figure 58 - ICX6610-48 and ICX6610-48P - Front, top and left side view with tamper evident label security seals 77
Figure 59 - ICX6610-48 and ICX6610-48P - Rear view with tamper evident label security seals 78
Figure 60 - ICX7450 with 24 ports - Front side 79
Figure 61 - ICX7450 with 48 ports - Front side 79
Figure 62 - ICX7450 - Top side 80
Figure 63 - ICX7450 - Rear side 81
Figure 64 - ICX7450 - Left side 81
Figure 65 - ICX7450 - Right side 81

1 Introduction

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.

The Brocade ICX 7450 Switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It offers market-leading stacking density with up to 12 switches (576x 1 GbE and 48x 10 GbE ports) per stack and combines chassis-level performance and reliability with the flexibility, cost-effectiveness, and "pay as you grow" scalability of a stackable solution. In addition, this stackable switch is the first in its class to offer 40 GbE uplinks, enabling enterprises to dramatically increase their network capacity while using their existing optical wire infrastructure.

2 Overview

The FIPS 140-2 validation includes hardware devices running the firmware version presented in Table 1. The module meets an overall FIPS 140-2 compliance of Security Level 2 with Design Assurance Level 3.

Table 2 and Table 3 list the devices included in this evaluation.

Table 2 lists the ten (10) Brocade ICX 6610 series devices, 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. 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 are listed in Table 2.

NOTE: Same components are used for assembly of (-I) and (-E) power supplies. Also, same components are used for assembly of (-I) and (-E) fan assemblies.

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 label security seals, supplied in FIPS Kit (Part Number: XBR- 000195) must be installed, as defined in Appendix A.

Table 3 lists the five (5) Brocade ICX 7450 series devices, referred collectively for the remainder of this document as ICX 7450 device (cryptographic module, or simply the module). Each ICX 7450 device is a fixed-port switch which provides three modular slots, four different optional port modules are offered for the Brocade ICX 7450. These modules are interchangeable and can be installed in any of the three modular slots within the Brocade ICX 7450. This environment is a multi-chip standalone cryptographic module. ICX 7450 offers a selection of PoE/non-PoE and AC/DC power supply options with front-to-back or back-to-front airflow cooling options. The DC power supply can be installed in either PoE or no-PoE switches. 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 7450 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 label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in Appendix A.

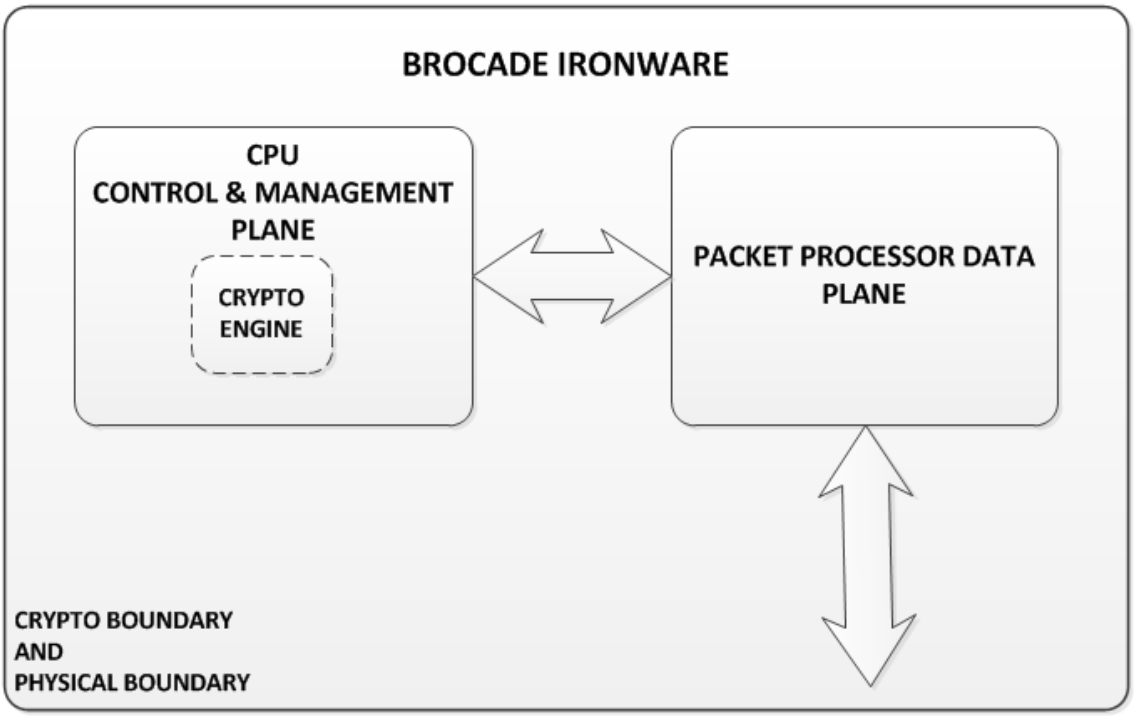

Figure 1 - Block diagram

3 FastIron Firmware

Each of the ICX series run a different firmware image which is built from the same source code. This firmware image includes the cryptographic functionality described under Section 7. The "–I" and "–E" 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. Otherwise, devices with similar SKUs are identical.

Firmware Version
IronWare R08.0.30b

Table 1 - Firmware Version

4 ICX 6610 Series

SKU	MFG Part Number	Brief Description
ICX6610-24-I	80-1005348-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow (“-I” in the SKU)
ICX6610-24-E	80-1005343-05	Stackable switch with 24 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow (“-E” in the SKU)
ICX6610-24P-I	80-1005349-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow (“-I” in the SKU)
ICX6610-24P-E	80-1005344-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow (“-E” in the SKU)
ICX6610-24F-I	80-1005350-04	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side intake airflow (“-I” in the SKU)
ICX6610-24F-E	80-1005345-04	Stackable switch with 24 100/1000 Mbps Small Form-Factor Pluggable (SFP) ports, power supply side exhaust airflow (“-E” in the SKU)
ICX6610-48-I	80-1005351-05	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side intake airflow (“-I” in the SKU)
ICX6610-48-E	80-1005346-05	Stackable switch with 48 10/100/1000 Mbps RJ-45 ports, power supply side exhaust airflow (“-E” in the SKU)
ICX6610-48P-I	80-1005352-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side intake airflow (“-I” in the SKU)
ICX6610-48P-E	80-1005347-06	Stackable switch with 24 10/100/1000 Mbps RJ-45 PoE+ ports, power supply side exhaust airflow (“-E” in the SKU)
XBR-000195	80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 2 - ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 2 through Figure 11 illustrate the ICX 6610-24 and ICX 6610-24P cryptographic modules (See Table 2 - ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules).

Figure 2 - Front and top side of the Brocade ICX 6610-24

Figure 3 - Back side of the Brocade ICX 6610-24

Figure 4 - Left side of the Brocade ICX 6610-24

Figure 5 - Right side of the Brocade ICX 6610-24

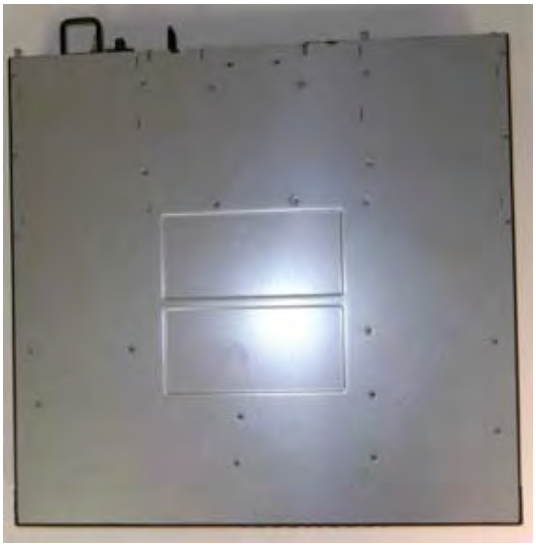

Figure 6 - Bottom side of the Brocade ICX 6610-24

Figure 7 - Front and top side of the Brocade ICX 6610-24P

Figure 8 - Back side of the Brocade 6610-24P

Figure 9 - Left side of the Brocade 6610-24P

Figure 10 - Right side of the Brocade 6610-24P

Figure 11 - Bottom side of the Brocade 6610-24P

Figure 12 through Figure 16 illustrates the ICX 6610-24F cryptographic modules (See Table 2 - ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules).

Figure 12 - Front and top side of the Brocade ICX 6610-24F

Figure 13 - Back side of the Brocade ICX 6610-24F

Figure 14 - Left side of the Brocade ICX 6610-24F

Figure 15 - Right side of the Brocade ICX 6610-24F

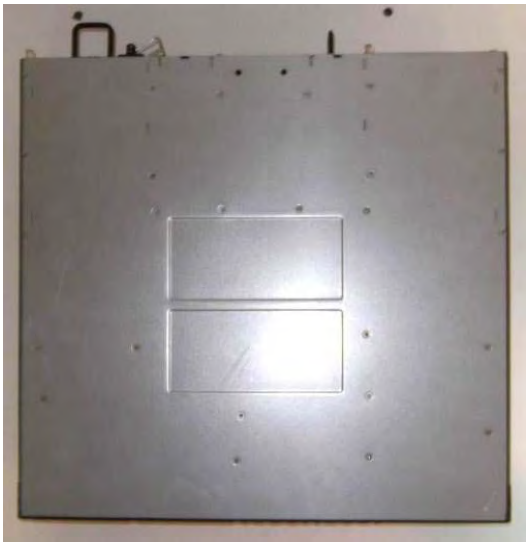

Figure 16 - Bottom side of the Brocade ICX 6610-24F

Figure 17 through Figure 26 illustrate the ICX 6610-48 and ICX 6610-48P cryptographic modules (See Table 2 - ICX 6610 Switch Family Part Numbers of Validated Cryptographic Modules).

Figure 17 - Front and top side of the Brocade ICX 6610-48

Figure 18 - Back side of the Brocade ICX 6610-48

Figure 19 - Left side of the Brocade ICX 6610-48

Figure 20 - Right side of the Brocade ICX 6610-48

Figure 21 - Bottom side of the Brocade ICX 6610-48

Figure 22 -Front and top side of the Brocade ICX 6610-48P

Figure 23 - Back side of the Brocade ICX 6610-48P

Figure 24 - Left side of the Brocade ICX 6610-48P

Figure 25 - Right side of the Brocade ICX 6610-48P

Figure 26 - Bottom side of the Brocade ICX 6610-48P

5 ICX 7450 Series

SKU	MFG Part Number	Brief Description
ICX7450-24	80-1008060-01	Brocade ICX7450 with 24-port 1 GbE, Modules, power supply & fan ordered separately
ICX7450-24P	80-1008061-01	Brocade ICX7450 with 24-port 1 GbE PoE+, Modules, power supply & fan ordered separately
ICX7450-48	80-1008062-01	Brocade ICX7450 with 48-port 1 GbE, Modules, power supply & fan ordered separately
ICX7450-48P	80-1008063-01	Brocade ICX7450 with 48-port 1 GbE PoE+, Modules, power supply & fan ordered separately
ICX7450-48F	80-1008064-01	Brocade ICX7450 with 48x 1GbE SFP ports. Modules, power supply & fan ordered separately.
XBR-000195	80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 3 - ICX 7450 Switch Family Part Numbers of Validated Cryptographic Modules

SKU	MFG Part Number	Brief Description
RPS15-E	80-1005261-04	Power supply - No-PoE 250 W AC with power-supply-side exhaust airflow
RPS15-I	80-1005259-04	Power supply - No-PoE 250 W AC with power-supply-side intake airflow
RPS16-E	80-1005262-03	Power supply - PoE 1000 W AC with power-supply-side exhaust airflow
RPS16-I	80-1005260-03	Power supply - PoE 1000 W AC with power-supply-side intake airflow
RPS16DC-E	80-1007165-03	Power supply - PoE 510 W DC with power-supply-side exhaust airflow
RPS16DC-I	80-1007166-03	Power supply - PoE 510 W DC with power-supply-side intake airflow
ICX7400-4X1GF	80-1008334-01	4-port 100M/1GbE SFP module
ICX7400-4X10GF	80-1008333-01	4-port 1/10GbE SFP/SFP+ module
ICX7400-4X10GC	80-1008332-01	4-port 1/10GbE 10GBASE-T Copper module
ICX7400-1X40GQ	80-1008331-01	1-port 40GbE QSFP+ for uplink or stacking module
ICX-FAN10-E	80-1008308-01	Power-supply-side exhaust airflow fan
ICX-FAN10-I	80-1008309-01	Power-supply-side intake airflow fan
N/A	123400000829A-R01	BLANK FAN TRAY ES4627BF-HPoE-FLF-08(SPATHA)-E LT
N/A	123400000830A-R01	BLANK PSU ES4627BF-HPoE-FLF-08(SPATHA)-E LT
N/A	123400000833A-R01	BLANK BRACKET ES4651BF-HPoE-FLF-08(SPATHA)-E LT

Table 4 - Components of the ICX 7450 Series

Switch Models	Components	Field Replaceable Units (max count)
ICX7450-24 See notes 1,2,3	Modules:	3 slots could be occupied with a combination of any of these modules. See table notes: ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (3)
	Power Supply:	RPS15-E (2), or RPS16DC-E (2), or RPS15-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)
ICX7450-24P See notes 1,2,3	Modules:	3 slots could be occupied with a combination of any of these modules. See table notes ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (3)
	Power Supply:	RPS16-E (2), or RPS16DC-E (2), or RPS16-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)
ICX7450-48 See notes 1,2,3,4	Modules:	3 slots could be occupied with a combination of any of these modules. See table notes ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (2)
	Power Supply:	RPS15-E (2), or RPS16DC-E (2), or RPS15-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)

Switch Models	Components	Field Replaceable Units (max count)
ICX7450-48P See notes 1,2,3,4	Modules:	3 slots could be occupied with a combination of any of these modules. See table notes ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (2)
	Power Supply:	RPS16-E (2), or RPS16DC-E (2), or RPS16-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)
ICX7450-48F See notes 1,2,3,4	Modules:	3 slots could be occupied with a combination of any of these modules. See table notes ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (2)
	Power Supply:	RPS15-E (2), or RPS16DC-E (2), or RPS15-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)

Table 5 - ICX 7450 Support Matrix

Table Notes:

1. Each Switch model shall be fully populated with a minimum of one Power Supply and one Fan unit, with every remaining slot populated with a Field Replaceable Unit (FRU) as per the table above.
2. Direction of the airflow for the Power Supply shall match the direction of the airflow of the Fan unit (e.g. ICX-FAN10-E shall be used in conjunction with RPS15-E, RPS16-E and RPS16DC-E).
3. The ICX7400-4X1GF (P/N: 80-1008334-01) FRU shall only be inserted in the front panel slot.
4. The ICX7400-1X40GQ (P/N: 80-1008331-01) FRU shall not be inserted in the front panel slot.

See Table 3, ICX 7450 Switch Family Part Numbers of Validated Cryptographic Modules.

Figure 27 through Figure 31 illustrates ICX7450-24 shown with optional Brocade ICX7400-4X10GF SFP+ uplink module.

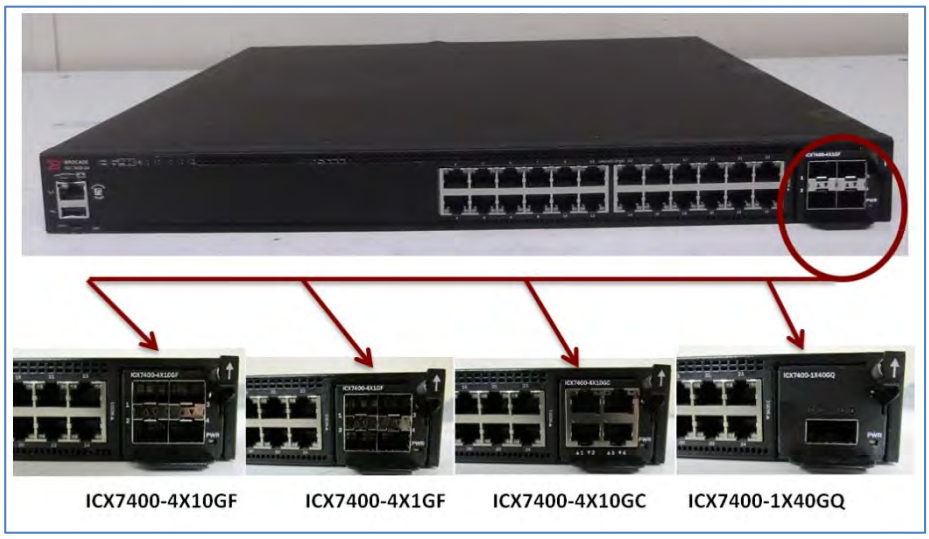

Figure 27 - Front/top side of the module ICX7450-24 with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ

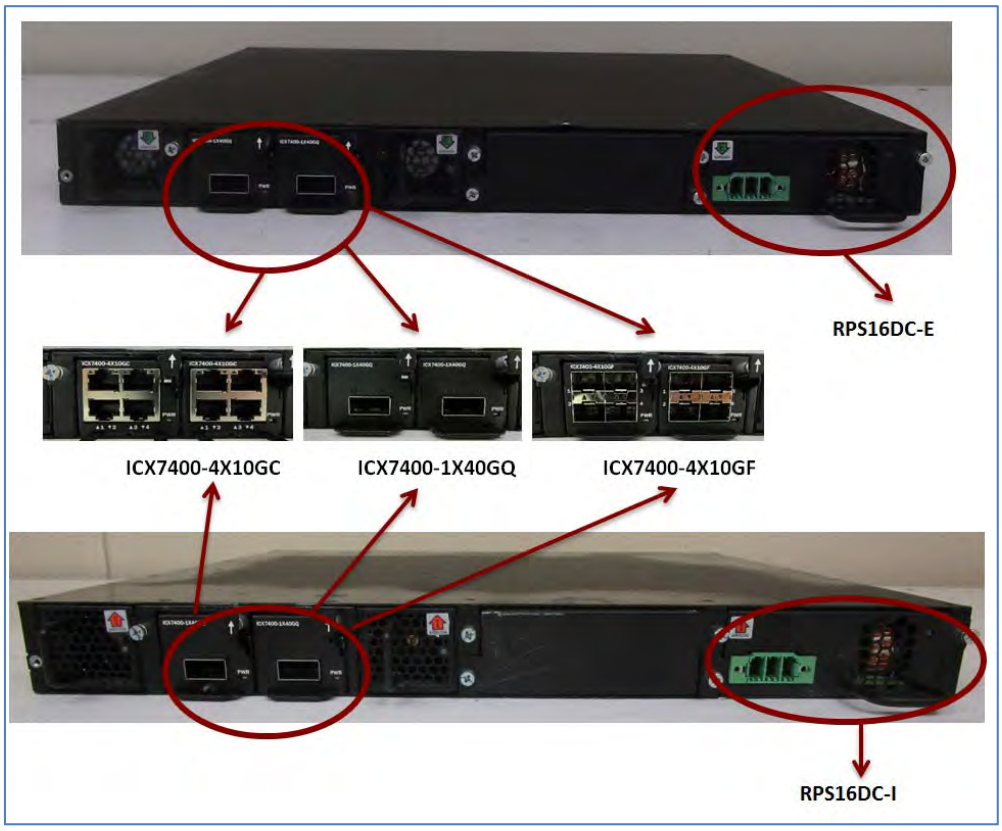

Figure 28 - Back side of the module ICX7450-24 with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 29 - Left side of the module ICX7450-24

Figure 30 - Right side of the module ICX7450-24

Figure 31 - Bottom side of the module ICX7450-24

Figure 32 through Figure 36 illustrates ICX7450-24P shown with optional Brocade ICX7400-1X40GQ QSFP+ uplink module.

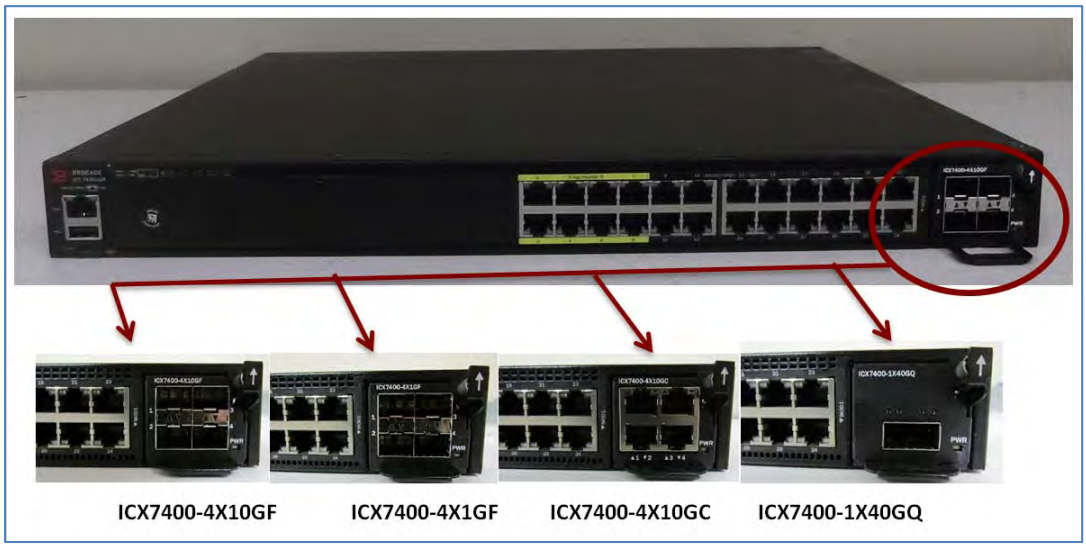

Figure 32 - Front/top side of the module ICX7450-24P with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

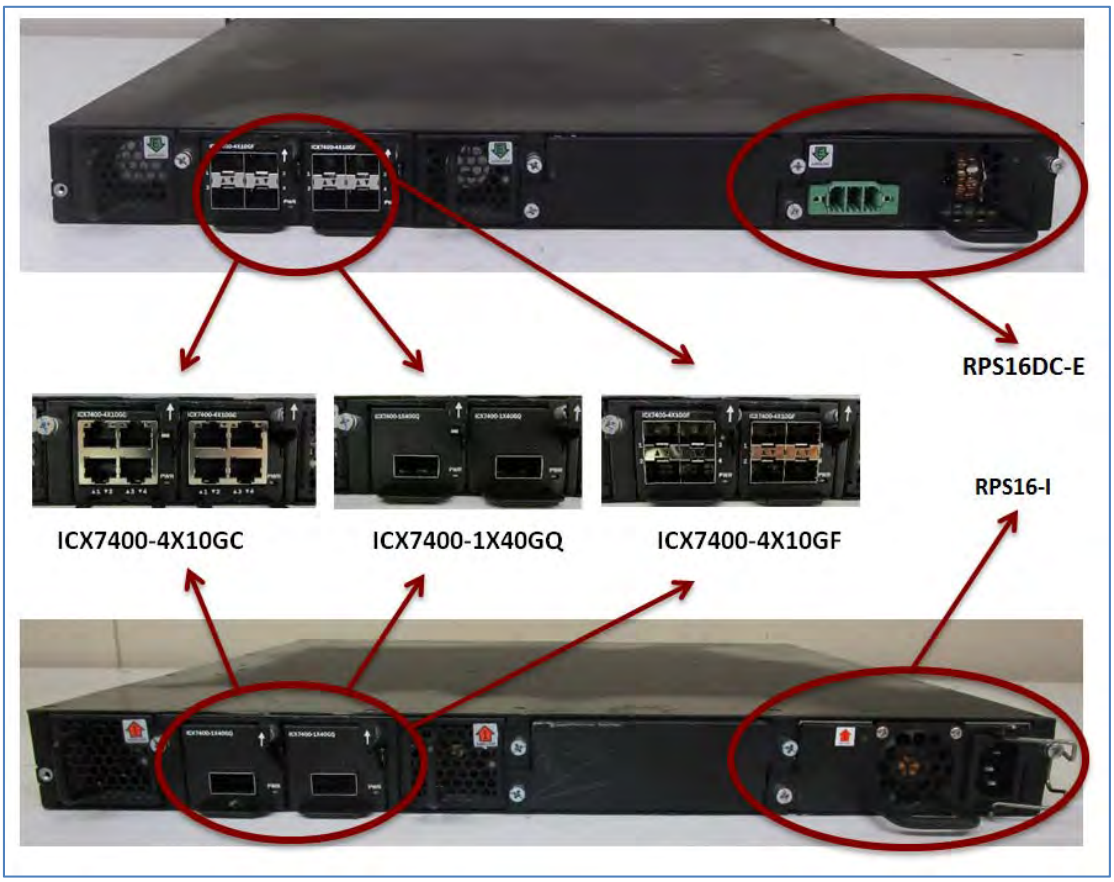

Figure 33 - Back side of the module ICX7450-24P with ICX7400-4X10GC, ICX7400-1X40GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 34 - Left side of the module ICX7450-24P

Next page →

Figure 35 - Right side of the module ICX7450-24P

Figure 36 - Bottom side of the module ICX7450-24P

Next page →

Figure 37 through Figure 41 illustrates ICX7450-48 shown with optional Brocade ICX7400-4X10GC 10GBase-T uplink module

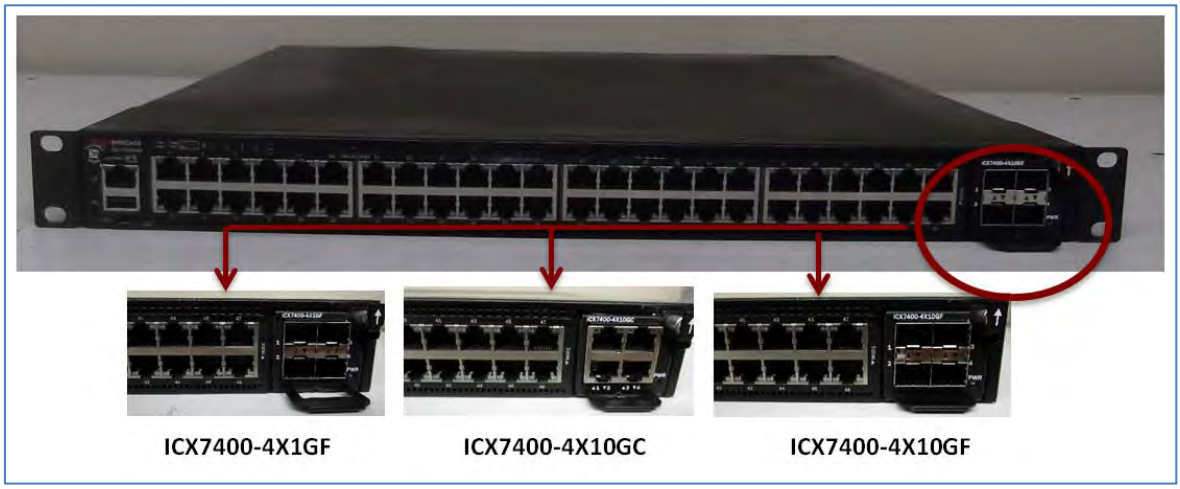

Figure 37 - Front/top side of the module ICX7450-48 with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF

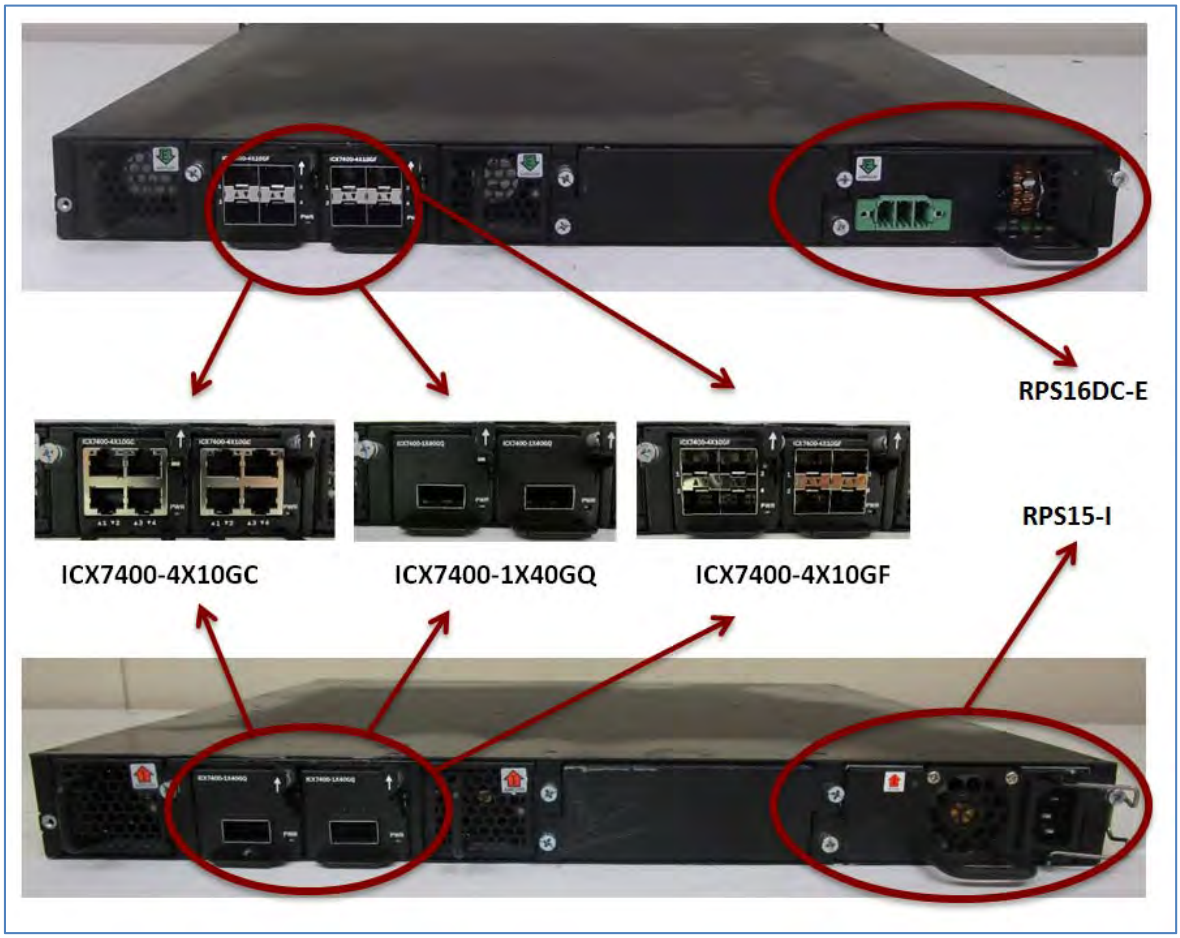

Figure 38 - Back side of the module ICX7450-48 with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 39 - Left side of the module ICX7450-48

Figure 40 - Right side of the module ICX7450-48

Figure 41 - Bottom side of the module ICX7450-48

Figure 42 through Figure 46 illustrates ICX7450-48P shown with optional Brocade ICX7400-4X10GF SFP+ uplink module.

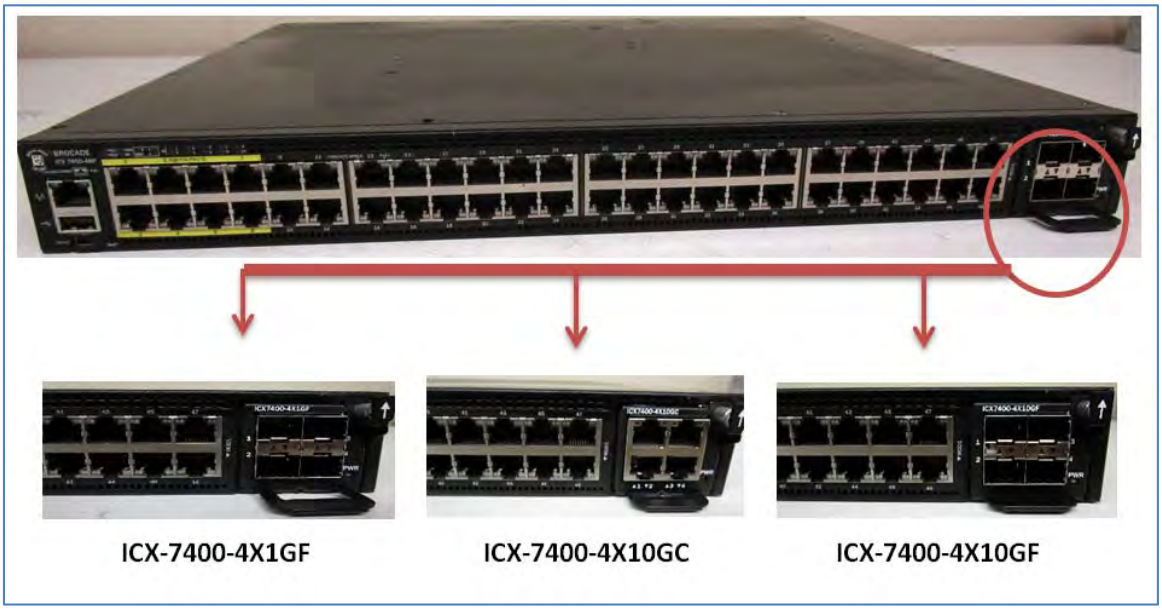

Figure 42 - Front/top side of the module ICX7450-48P with ICX74004X1GF, ICX7400-4X10GC and ICX7400-4X10GF

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

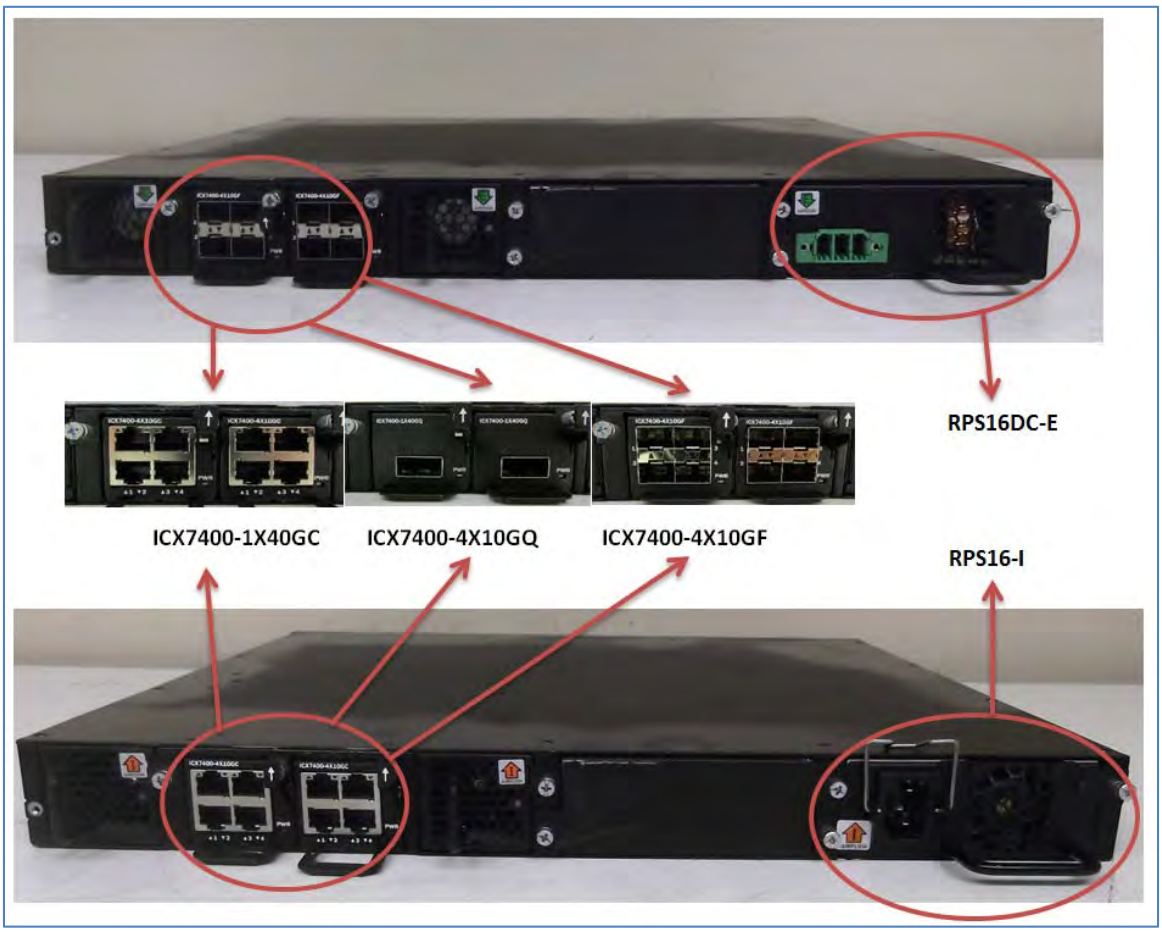

Figure 43 - Back side of the module ICX7450-48P with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 44 - Left side of the module ICX7450-48P

Figure 45 - Right side of the module ICX7450-48P

Figure 46 - Bottom side of the module ICX7450-48P

Next page →

Figure 47 through Figure 51 illustrates ICX7450-48F shown with optional Brocade ICX 7400-4X10GF SFP+ uplink module.

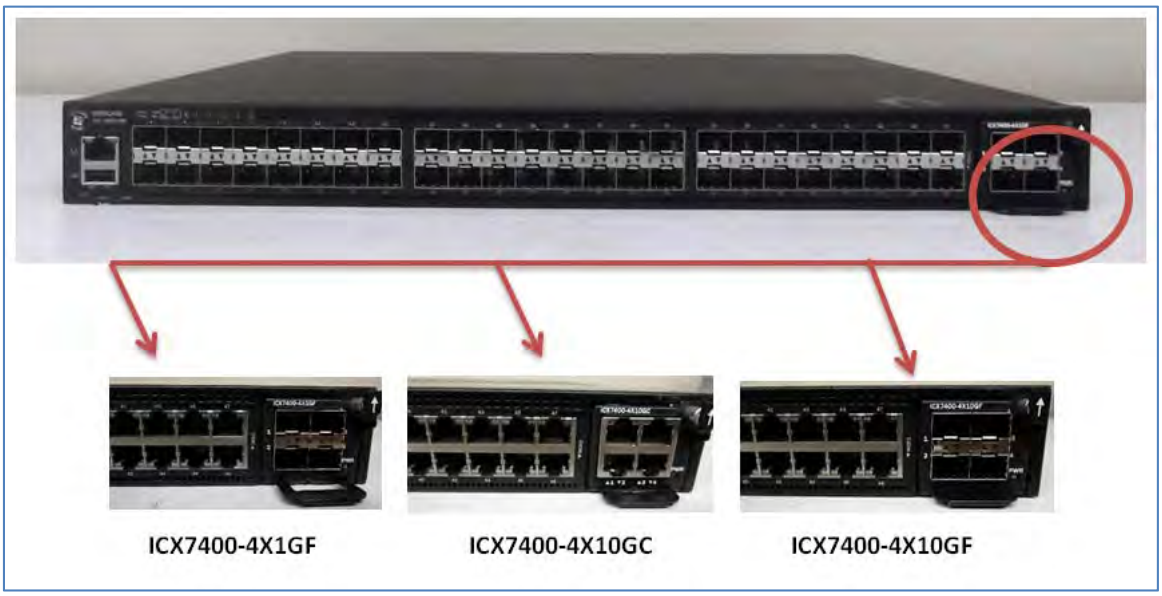

Figure 47 - Front/top side of the module ICX7450-48F with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF

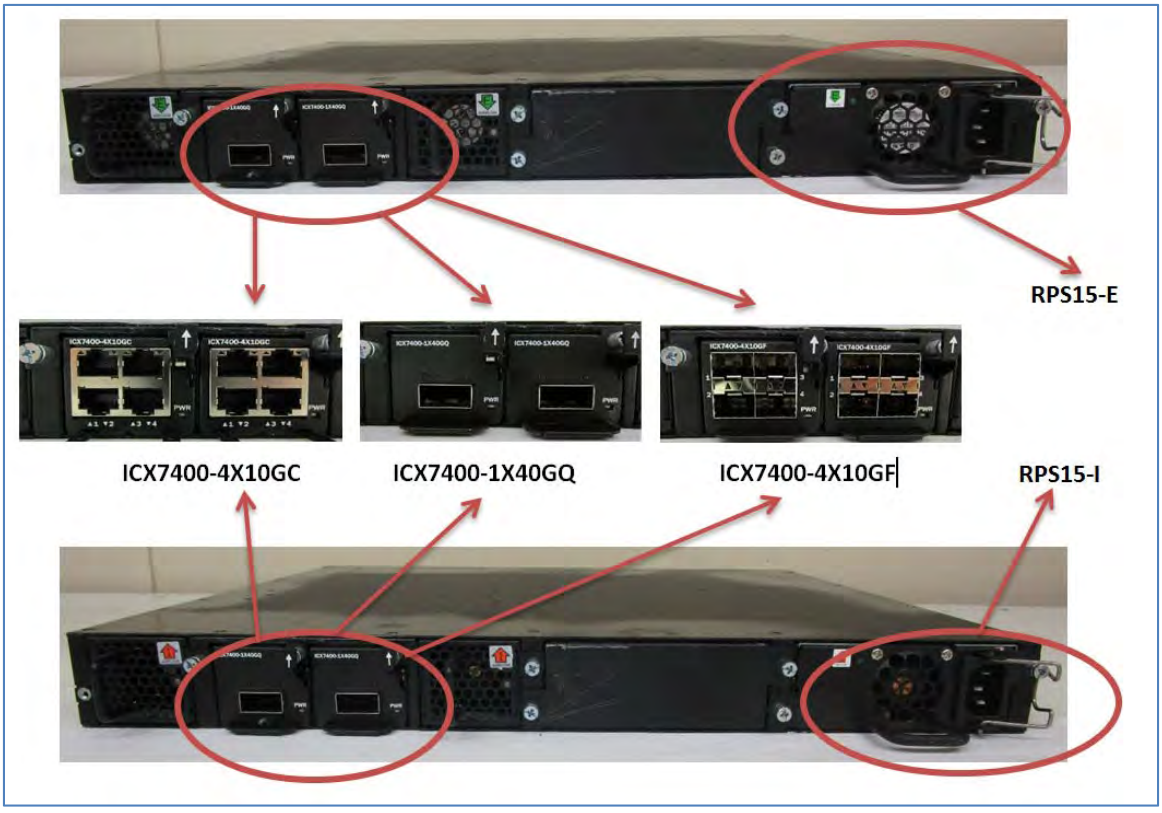

Figure 48 - Back side of the module ICX7450-48F with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 49 - Left side of the module ICX7450-48F

Figure 50 - Right side of the module ICX7450-48F

Figure 51 - Bottom side of ICX7450-48F

6 Ports and Interfaces

6.1 ICX 6610 Series

Each ICX 6610 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

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).

Table 6 summarizes the network ports provided by each ICX 6610 model. Table 7 shows the correspondence between the physical interfaces of ICX 6610 devices and the logical interfaces defined in FIPS 140-2.

ICX 6610 Series Physical Ports

Model	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 ports1	AC inlet2	Reset	Out of band management ports	LEDs												
								Ethernet		PoE+			System Status							
								Speed	Status	Speed	Status	SFP/SFP+	PSU	PSU	Diag	XL	XL	MS	XL2-XL5	XL7-XL10	StackD3
ICX6610-24F-I, ICX6610-24F-E	8	N/A	24	4	2	1	2	N/A	N/A	N/A	N/A	40	1	1	1	1	1	1	1	1	10
ICX6610-24-I, ICX6610-24-E	8	24	N/A	4	2	1	2	24	24	N/A	N/A	8	1	1	1	1	1	1	1	1	10
ICX6610-24P-I, ICX6610-24P-E	8	24	N/A	4	2	1	2	N/A	N/A	24	24	8	1	1	1	1	1	1	1	1	10
ICX6610-48-I, ICX6610-48-E	8	48	N/A	4	2	1	2	48	48	N/A	N/A	8	1	1	1	1	1	1	1	1	10
ICX6610-48P-I, ICX6610-48P-E	8	48	N/A	4	2	1	2	N/A	N/A	48	48	8	1	1	1	1	1	1	1	1	10

Table 6 - ICX 6610 Series Physical Ports

Mapping ICX 6610 physical ports to logical interfaces

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	Control input, Status output
Reset	Control input
LED	Status output

Table 7 - ICX 6610 Port mapping to logical interface

6.2 ICX 7450 Series

An ICX 7450 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7450 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7450 device has one RJ-45 network management port, one mini USB serial management port, and one USB storage port on the front panel

Table *8* shows the correspondence between the physical interfaces of an ICX 7450 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
QSFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
DC socket	Power
Console Port	Control input, Status output
Out of band management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 8 - ICX 7450 Port mapping to logical interface

Table 9 through Table 16 summarizes the physical port LED status provided by ICX 7450 devices.

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Port link is up in 10/100 Mbps mode. No traffic is being transmitted
Blinking amber	There is 10/100 Mbps traffic and packets are being transmitted or received
Steady green	Port link is up in 1 Gbps mode. No traffic is being transmitted
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 9 - Management port (10/100/1000 Mbps) status LED

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 100 Mbps mode.
Blinking amber	There is 100 Mbps traffic and packets are being transmitted or received
Steady green	Link is up in 1 Gbps mode
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 10 - 100/1000 Mbps RJ-45 port LEDs

LED state	Status of hardware
Steady green	Port is providing POE power to a connected device.
Off	Port is not providing PoE power

Table 11 - 100/1000 Mbps RJ-45 PoE LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 100 Mbps mode.
Blinking amber	There is 100 Mbps traffic and packets are being transmitted or received
Steady green	Link is up in 1 Gbps mode
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 12 - 100/1000 Mbps SFP port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 1 Gbps mode.
Blinking amber	There is 1 Gbps traffic and packets are being transmitted or received
Steady green	Link is up in 10 Gbps mode
Blinking green	There is 10 Gbps traffic and packets are being transmitted or received

Table 13 - 1/10 Gbps RJ-45 port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 1 GbE mode.
Blinking amber	There is 1 GbE traffic and packets are being transmitted or received
Steady green	Link is up in 10 GbE mode
Blinking green	There is 10 GbE traffic and packets are being transmitted or received

Table 14 - 1/10 GbE SFP+ module port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady green	Link is up in 40 GbE mode (MOD2 data uplink mode or MOD3/MOD4 stacking mode)
Blinking green	There is 40 GbE traffic and packets are being transmitted or received

Table 15 - 40 GbE mode QSFP+ module port LEDs (left-side LED)

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Port lane link is up in 10 GbE mode (MOD2 data uplink mode)
Blinking amber	There is 10 GbE traffic and packets are being transmitted or received

Table 16 - 4x10 GbE mode QSFP+ module port LEDs

Table 17 through Table 22 summarizes the system LED status provided by ICX 7450 devices.

LED state	Status of hardware
Off (no light)	System is off or there is no power
Steady green	PSU is on and functioning properly
Steady amber	PSU is missing power or in a faulty state (such as PSU fan failure)

Table 17 ICX 7450 - PSU1 and PSU2 LEDs

LED state	Status of hardware
Off (no light)	Diagnostic is off
Blinking green	System self-diagnostic test is in progress
Steady green	System self-diagnostic test has successfully completed
Steady amber	System self-diagnostic test has detected a fault

Table 18 - ICX 7450 - DIAG LED

LED state	Status of hardware
Off (no light)	Stacking mode is enabled and the switch is a stack member operating in slave mode, or the switch is operating in standalone mode.
Blinking green	Device is initializing
Steady green	Stacking mode is enabled and the switch is the stack master
Steady amber	Stacking mode is initializing and the switch is the standby controller
Blinking amber	Stacking mode is initializing and the switch is in stacking master arbitration/selection state.

Table 19 - ICX 7450 - MS LED

LED state	Status of hardware
Off (no light)	Module is used for stacking or no module is installed. For stacking modules, this means that stacking mode is enabled and the switch is a stack member, or the switch is operating in stand-alone mode
Steady green	Module is operating normally. For stacking modules, this means that stacking mode is enabled and the switch is a stack master

Table 20 - ICX 7450 - MOD LED

LED state	Status of hardware
Steady green	Indicates stack unit identifier. (Unit numbers 11 and 12 are shown by using the 10+ LED in combination with the 1 or 2 LED.)

Table 21 - ICX 7450 - Stack ID LEDs

LED state	Status of hardware
Off (no light)	Module is not receiving power.
Steady green	Module is on and functioning properly
Steady amber	Module is on and booting up

Table 22 - ICX 7450 - Module Power LED (all media/stacking modules)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7 Modes of Operation

ICX 6610 devices and ICX 7450 devices (aka Brocade cryptographic modules) have two modes of operation: FIPS Approved mode and non-Approved mode. Section 7.3 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 10.3 FIPS Approved Mode describes how to invoke FIPS Approved mode.

7.1 Module Validation Level

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

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

Table 23 - Security Requirements and Levels

7.2 Roles

In FIPS Approved mode, Brocade cryptographic modules support four roles: Crypto Officer, Port Configuration Administrator, User and MACsec Peer:

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. The Crypto Officer is the only role that can perform firmware loading.

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).

4. MACsec Peer - A peer device which establishes a MACsec connection with the cryptographic module using AES 128-bit pre-shared key.

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

Section 8.2 describes the authentication policy for user roles.

7.3 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a power-cycle. They can also view the module status by entering CLI "*`fips show`*" command.

For all other services, an operator must authenticate to the device as described in section 8.2 Authentication. Brocade cryptographic modules provide services for remote communication (SSHv2, Secure Web Management over TLS v1.0/v1.1, TLS v1.2, 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 *24* summarizes the available FIPS Approved cryptographic functions. Table 25 lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

Label	Cryptographic Algorithms
AES	Advanced Encryption Algorithm (CBC, CMAC, CFB, GCM, and Key Wrap modes)
SHA	Secure Hash Algorithm
HMAC	Keyed-Hash Message Authentication code
DRBG	Deterministic Random Bit Generator
RSA	Rivest Shamir Adleman Signature Algorithm
CVL	SSHv2, TLS v1.0/1.1, TLS v1.2, and SNMPv3 Key Derivation Function
KBKDF	SP800-108 KDF

Table 24 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode

Table, below, lists all FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode.

Label	Cryptographic Algorithms
KW	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
HMAC-MD5	Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
HMAC-MD5	Used in the TLS v1.0 KDF in FIPS mode as per SP800-135 (HMAC-MD5 is not exposed to the operator)
MD5	Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
NDRNG	Generation of seeds for DRBG
DH KA	Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)

Table 25 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode

Table, below, lists all FIPS non-Approved cryptographic functions and protocols only available in non-FIPS Approved Mode.

Role	Service / Function	Description
This is not a user accessible service	HTTPS Cipher Suites	Hyper Text Transport Protocol in secure connection mode
Crypto Officer Role, User Role	HTTP	Hyper Text Transport Protocol (plaintext; no cryptography)
Crypto Officer Role, User Role	SSHv2	2-key Triple-DES (non-compliant), 3-key Triple-DES (non-compliant)
Crypto Officer Role, User Role	SNMP { Simple Network Management Protocol v1, v2 and v3 with MD5 / DES, AES (non-compliant) / SHA-1 (non-compliant) }	MD5 and DES, AES (non-compliant) / SHA-1 (non-compliant), SNMPv1, SNMPv2c and SNMPv3 (non-compliant) in noAuthNoPriv, authNoPriv modes Modes: DES in authPriv mode for SNMPV3 (non-compliant) Key sizes: DES 56 bits, AES-128 (non-compliant)

Role	Service / Function	Description
Crypto Officer Role, User Role	TACACS	Terminal Access Controller Access Control System is an authentication protocol which allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. Mode: HMAC-MD5
Crypto Officer Role	TFTP (Trivial File Transfer Protocol)	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. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	“Two way encryption”	Base64
This is not a user accessible service	MD5	Message Digest 5 algorithm is used as cryptographic hash function to check for verification of data integrity and wide variety of cryptographic applications Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	Syslog	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VSRP	Virtual Switch Redundancy Protocol Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VRRP/VRRP-E	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)

Role	Service / Function	Description
Crypto Officer Role, User Role	MSTP	Multiple Spanning Tree Protocol Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	NTP (Authentication using MD5)	Network Time Protocol Modes: MD5 and SHA-1 (non-compliant) for authentication Key sizes: 20 bytes
Crypto Officer Role, User Role	BGP	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	AES-192 (non-compliant)	AES-192 (non-compliant) encryption/decryption is only available in non-FIPS mode
This is not a user accessible service	DSA (non-compliant)	DSA (non-compliant) digital signature generation/verification only available in non- FIPS mode

Table 26 - FIPS non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7.4 User Role Services

7.4.1 SSHv2

This service provides a secure session between a Brocade cryptographic module and an SSHv2 client using SSHv2 protocol. Brocade cryptographic modules authenticate an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface.

Brocade cryptographic modules support three kinds of SSHv2 client authentication: password, client public key and keyboard interactive. For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The Brocade cryptographic module authenticates operator with passwords stored on the device, on a TACACS+ server, or on a RADIUS server. Section 8.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one step ahead. It allows multiple challenges to be issued by the Brocade cryptographic module, using the backend RADIUS or TACACS+ server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the Brocade cryptographic module.

SSHv2 supports Diffie-Hellman (DH) to configure the modulus size on the SSHv2 server for the purpose of key- exchange.

Maximum number of concurrent SSHv2 user sessions supported is 5.

The following encryption algorithms are available for negotiation during the key exchange with an SSHv2 client:

- AES-CBC with a 128-bit key (aes128-cbc),
- AES-CBC with a 256-bit key (aes256-cbc),

All secure hashing is done with SHA-256.

The following MAC algorithms are available for negotiation during the key exchange with an SSHv2 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 the 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`* in addition to *`show`* commands.

7.4.2 HTTPS

This service provides a graphical user interface for managing a Brocade cryptographic module over a secure communication channel. Using a web browser, an operator connects to a designated management port on a Brocade cryptographic module. The device negotiates a TLS v1.0/1.1 and v1.2 connection with the browser and authenticates the operator. The device uses HTTP over TLS v1.0/1.1 and v1.2 with cipher suites TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, and TLS_DHE_RSA_WITH_AES_256_CBC_SHA256. Brocade switches have the ability to generate RSA 2048 certificates signed with SHA 256.

Maximum number of concurrent HTTPS user sessions supported is 8.

In User role, after successful login, the default HTML page is the 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 re-enter 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.

7.4.3 SNMP

SNMPv1 and SNMPv2 services are disabled in FIPS mode and the SNMPv3 service with authentication as MD5 and privacy as DES are also disabled. The SNMPv3 service within User role allows read-only access to the SNMP MIB within the FastIron device. The device does not provide SNMP MIB access to CSPs when operating in FIPS Approved mode. All other MIB objects are made available for use in approved FIPS mode. These other MIB objects provide capability to monitor the various functional entities in the module which are non-security relevant.

7.4.4 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 a Brocade cryptographic module 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 the same as the list mentioned in the SSHv2 service.

7.4.5 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

7.5 Port Configuration Administrator Role Services

7.5.1 SSHv2

This service is described in Section 7.4.1 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 7.4.1. 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.

7.5.2 HTTPS

This service is described in Section 7.4.2 above.

Like the 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.

7.5.3 SNMP

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

7.5.4 Console

This service is described in Section 7.4.4 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 the same as those mentioned in the SSHv2 service.

7.5.5 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

Next page →

7.6 Crypto Officer Role Services

7.6.1 SSHv2

In addition to the two methods of authentication, password and keyboard interactive, described in Section 7.4.1, SSHv2 service in this role supports RSA 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 SSHv2. 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 (including enabling and disabling MACsec on a per-port basis). This role has full read and write access to the Brocade cryptographic module.

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

The Crypto Officer can perform zeroization by invoking the firmware command "`fips zeroize all`" or session termination.

7.6.2 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 SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on Brocade cryptographic modules 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.

7.6.3 HTTPS

This service is described in Section 7.4.2 above.

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.

7.6.4 SNMP

This service is described in Section 7.4.3 above. The SNMP service within Crypto Officer Role allows read- write access to only Non-Security Relevant elements of the SNMP MIB within the FastIron device.

7.6.5 Console

Logging in through the CLI service is described in Section 7.4.4 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the Brocade cryptographic module. 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 SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access; afterwards the operator may securely import additional pairs of RSA host keys as needed over a secured SSHv2 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 SSHv2 connection), and enable the HTTPS server.

NOTE: The cryptographic module "does not" support DSA key generation in FIPS mode.

7.6.6 NTP

The NTP [same as NTPv4] Network Time Protocol can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server. Symmetric key scheme is supported for authentication.

NTPv4 specification (RFC-5905), allows any one of possibly 65,534 message digest keys (excluding zero), each distinguished by a 32-bit key ID, to authenticate an association. The servers and clients involved must agree on the key ID, key type and key to authenticate NTP packets.

NTP service with MD5 key authentication is disabled in FIPS mode.

NTPv4 service with SHA1 key authentication is available upon configuration in FIPS mode.

7.7 MACsec Peer Role Services

7.7.1 MACsec

Establishes and maintains MACsec sessions with the cryptographic module using AES 128-bit pre-shared keys.

8 Policies

8.1 Security Rules

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

1) The cryptographic module provides role-based authentication.

2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSP).

3) The cryptographic module performs the following tests:

    a) Power up Self-Tests:

i) Cryptographic Known Answer Tests (KAT):

(1) Triple-DES KAT (encrypt)

(2) Triple-DES KAT (decrypt)

(3) AES-128,192,256-bit key sizes KAT (encrypt) in CBC, ECB, CTR and CFB modes

(4) AES-128,192,256-bit key sizes KAT (decrypt) in CBC, ECB, CTR and CFB modes

(5) AES-CMAC KAT

(6) AES-KW KAT

(7) SHA-1,256,384,512 KAT (Hashing)

(8) HMAC-SHA-1,256 KAT (Hashing)

(9) RSA 2048 bit key size KAT (encrypt)

(10) RSA 2048 bit key size KAT (decrypt)

(11) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature generation)

(12) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature verification)

(13) DRBG KAT

(14) SP800-135 TLS v1.0 KDF KAT

(15) SP800-135 SSHv2 KDF KAT

(16) SP800-135 TLS v1.2 KDF KAT

(17) SP800-135 SNMPv3 KDF KAT

(18) SP800-108 KBKDF KAT

(19) AES-GCM KAT

ii) Firmware Integrity Test (CRC 32)

iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

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

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

```
Crypto Module Failed < Reason String >
```

b) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on NDRNG

ii) Continuous Random Number Generator test – performed on DRBG

iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

v) Firmware Load Test: RSA 2048 bit, SHA-256 Signature Verification

vi) Alternating Bypass Test

vii) Manual Key Entry Test: N/A

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

5) Data output to services defined in Section 7.3 Services is inhibited during key generation, self-tests, zeroization, and error states.

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

7) As per FIPS 140-2 Implementation Guidance D.11, Brocade hereby states that the following protocols have not been reviewed or tested by the CAVP or CMVP:
   a) TLS v1.0/1.1
   b) SSHv2
   c) TLS v1.2
   d) SNMPv3

8.1.1 FIPS Fatal Cryptographic Module Failure

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

```
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.

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

In order to operate a Brocade cryptographic module 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 a Brocade cryptographic module.

Brocade cryptographic modules shall use a FIPS Approved random number generator implementing Algorithm CTR_DRBG based on hash functions.

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

Brocade cryptographic modules shall use FIPS Approved key generation methods:

1) RSA public and private keys in accordance with [ANSI X9.31]

Brocade cryptographic modules shall test prime numbers generated for RSA keys using Miller-Rabin test. See [ANSI X9.31]

Brocade cryptographic modules shall use Approved key establishment techniques:

1) Diffie-Hellman
2) RSA Key Wrapping
3) AES Key Wrapping

Brocade cryptographic modules shall restrict key entry and key generation to authenticated roles.

Brocade cryptographic modules shall not display plaintext secret or private keys. The device shall display "…" in place of plaintext keys.

Brocade cryptographic modules shall use automated methods to realize session keys for SSHv2 and HTTPS. Brocade cryptographic modules shall only perform "get" operations using SNMP.

8.2 Authentication

Brocade cryptographic modules support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS+, RADIUS and local configuration database. Moreover, Brocade cryptographic modules 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, SSHv2, Web and SNMP) and the order in which the device tries one or more of the following authentication methods:

1) Line Password Authentication,
2) Enable Password Authentication,
3) Local User Authentication,
4) RADIUS Authentication with exec authorization and command authorization, and
5) TACACS+ Authentication with exec authorization and command authorization

6) Pre-shared keys

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.

Brocade cryptographic modules allow multiple concurrent operators through SSHv2 and the console, only limited by the system resources.

8.2.1 Line Password Authentication Method

The Line Password Authentication method uses the Telnet password to authenticate an operator.

To use Line Password Authentication, a Crypto Officer must set the Telnet password. Please note that when operating in FIPS mode, Telnet is disabled and Line Password Authentication is not available.

8.2.2 Enable Password Authentication Method

The Enable Password Authentication 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 select the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use Enable Password Authentication, a Crypto Officer must set the password for each privilege level.

8.2.3 Local Password Authentication Method

The Local Password Authentication Method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. Brocade cryptographic modules assign the role associated with the user name to the operator when authentication is successful.

To use Local Password Authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

8.2.4 RADIUS Authentication Method

The RADIUS Authentication method uses one or more RADIUS servers to verify user names and passwords. Brocade cryptographic modules prompt 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, a Brocade cryptographic module will send the user name and password information to the next configured RADIUS server.

Brocade cryptographic modules support additional command authorization with RADIUS Authentication. The following events occur when RADIUS command authorization takes place.

1) A user previously authenticated by a RADIUS server enters a command on a Brocade cryptographic module.

2) A Brocade cryptographic module looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.

3) If the command belongs to a privilege level that requires authorization, the Brocade cryptographic modules 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 Brocade cryptographic module. 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 Brocade cryptographic module.

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

8.2.5 TACACS+ Authentication Method

The TACACS+ Authentication Method uses one or more TACACS+ servers to verify user names and passwords. For TACACS+ Authentication, Brocade cryptographic modules prompt 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.

8.2.6 Pre-shared keys Method

The MACsec Peer role establishes and maintains MACsec sessions using AES 128-bit pre-shared keys that are configured by the Crypto Officer.

8.2.7 Strength of Authentication

This section describes the strength of each authentication method.

8.2.7.1 MACsec Peer Role (only)

The MACsec Peer Role is assumed implicitly as follows:

Specifically in reference to MACsec Peer Role only, the probability of a successful random guess of the AES 128-bit pre-shared key is 1/ 2^128 for a random attempt, which is less than 1/1,000,000. The module only supports a maximum of 60 attempts during a one minute period due to the timing of the protocol. This means that the probability of false authorization with multiple consecutive random attempts during a one minute period is 60 / 2^128, which is less than 1/100,000.

8.2.7.2 All other roles (except MACsec Peer Role)

All other users except for the MACsec Peer Role can utilize all other available authentication techniques for the purpose of authentication.

Brocade cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 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 60/80^8 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 which is less than 1/100,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

For the SNMPv3 secret used for authentication, the module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

For the SNMPv3 secret used for privacy, the module supports minimum 12 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^12 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^12 which is less than 1/100,000.

For the NTP secret, the module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

Next page →

8.2.8 Access Control Policy and CSP & Public Key access

Table *27* and Table 28 summarize the access operators in each role have to critical security parameters. The table entries have the following meanings:

1) r – Operator can read the value of the item,
2) w - Operator can write a new value for the item,
3) x - Operator can use the value of the item without direct access (for example encrypt with an encryption key)
4) d - Operator can delete the value of the item (zeroize).

Roles & Services / CSP & Public Keys		User					Port Configuration Administrator				Crypto Officer					
		SSHv2	HTTPS	SNMP	Console	NTP	SSHv2	HTTPS	Console	NTP	SSHv2	SCP	HTTPS	SNMP	Console	NTP
1	SSHv2 Host RSA Private Key (2048 bit)	x					x				xwd	x			wd	
2	SSHv2 DH Private Key (2048 bit)	x					x				xwd	x			wd	
3	SSHv2 DH Shared Secret Key (2048 bit)	x					x				xd	x			xd	
4	SSHv2/SCP Session Keys (128 and 256 bit AES CBC)	x					x				xd	x			xd	
5	SSHv2/SCP Authentication Key (HMAC-SHA-1)	x					x				xd	x			xd	
6	SSHv2 KDF Internal State	x					x				xd	x			xd	
7	TLS Host RSA Private Key (RSA 2048 bit)		X					x			rwd		x		rwd	
8	TLS Pre-Master Secret		X					x					x		xd	
9	TLS Master Secret		X					x					x		xd	
10	TLS KDF Internal State		X					x			xd		x		xd	
11	TLS Session Key		X					x					x		xd	

Roles & Services / CSP & Public Keys		User					Port Configuration Administrator				Crypto Officer					
		SSHv2	HTTPS	SNMP	Console	NTP	SSHv2	HTTPS	Console	NTP	SSHv2	SCP	HTTPS	SNMP	Console	NTP
12	TLS Authentication Key		X					x					xd		xd	
13	DRBG Seed	x	X				x	x			xd	x	x		xd	
14	DRBG Value V	x	X				x	x			xd	x	x		xd	
15	DRBG Key	x	X				x	x			xd	x	x		xd	
16	DRBG Internal State	x	X				x	x			xd	x	x		xd	
17	User Password	x	X	x	x						xrwd	xrwd	xrwd	x	xrwd	
18	Port Administrator Password						x	x	X		xrwd	xrwd	rwd		xrwd	
19	Crypto Officer Password										xrwd	xrwd	xrwd		xrwd	
20	RADIUS Secret	x	X		x		x	x	X		xrwd	xrwd	xrwd		xrwd	
21	TACACS+ Secret	x	X		x		x	x	X		xrwd	xrwd	xrwd		xrwd	
22	Firmware Integrity / Firmware Load RSA Public Key										xd		x		xd	
23	SSHv2 Host RSA Public key	x					x				xrwd	xrw			rwd	
24	SSHv2 Client RSA Public Key	x					x				xrwd	xrwd			xrwd	
25	SSHv2 DH Public Key	x					x				xd	x			xd	
26	SSHv2 DH Peer Public Key	x					x				xd	x			xd	

Roles & Services / CSP & Public Keys		User					Port Configuration Administrator				Crypto Officer					
		SSHv2	HTTPS	SNMP	Console	NTP	SSHv2	HTTPS	Console	NTP	SSHv2	SCP	HTTPS	SNMP	Console	NTP
27	TLS Host Public Key (RSA 2048 bit)		X					x			rwd		x		rwd	
28	TLS Peer Public Key (RSA 2048 bit)		X					x			rwd		x		Rwd	
29	SNMPv3 secret	r		r	r		r		R		rwd	rwd		r	rwd	
30	NTP secret	r			r	r	r		R	r	rwd	rwd		r	rw	R w d
31	CAK										rwd	rwd			rwd	
32	CKN										rwd	rwd			rwd	
33	ICK										d				d	
34	KEK										d				d	
35	SAK										dx				dx	
36	SP800-108 KDF Internal State										rwd				rwd	

Table 27 - Access Control Policy and CSP & Public Key access

CSP		MACsec Peer
		MACsec Service
1	CAK	xd
2	CKN	xd
3	ICK	xd
4	KEK	xd
5	SAK	rwxd
6	SP800-108 KDF Internal State	xd

Table 28 - Access Control Policy and CSP access for MACsec Peer role

9 Physical Security

In order for an ICX 6610 device or ICX 7450 device to meet FIPS 140-2 Level 2 Physical Security requirements the Crypto Officer must install tamper evident label security seals. Tamper evident label security seals are available for order from Brocade under FIPS Kit (Part Number: XBR-000195). The Crypto Officer shall follow the Brocade FIPS Security Seal application procedures defined in section 13 (Appendix A: Tamper Evident Label application) 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 label security 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 Crypto 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: Tamper Evident Label application of this Security Policy document for specific tamper evident seal application instructions.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10 Description of FIPS Approved Mode

This section describes:

A. FIPS Approved mode, section 10.1, describes:
   - This section describes required actions before you can use the module in FIPS Approved mode of operation
   - The nature of operational conditions in the module while operating in FIPS Approved mode.

B. Displaying mode status, section 10.2, provides details on how to examine the status for the module's mode of operation.

C. Invoking FIPS approved mode, section 10.3, describes the required steps in order to invoke the FIPS approved mode on the module.

10.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that places a Brocade cryptographic module in FIPS Approved mode.

The first required action is to apply tamper evident label security seals to the module. See, section 13, Appendix A: Tamper Evident Label application, for specific details and instructions for each module.

FIPS Approved mode disables the following:

1) Telnet access including the telnet server command
2) Command `ip ssh scp disable`
3) TFTP access
4) SNMP access to CSP MIB objects
5) Access to all commands within the monitor mode
6) HTTP access including the web-management http command
7) Port 280
8) HTTPS SSL 3.0 access Command web-management allow-no-password

Entering FIPS Approved mode also clears:

1) Protocol shared secret and host passwords
2) SSHv2 RSA host keys
3) HTTPS RSA host keys and certificate

FIPS Approved mode enables:

1) SCP
2) HTTPS TLS v1.0/1.1 and v1.2

Following table, below, lists all algorithm certificates for the ICX 6610 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB, CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2697, #3139 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
AES-CMAC	AES-CMAC	#3008
AES Key Wrap	AES-KW	#2984
AES GCM	GCM	#1276
AES	ECB (128 bits)	#1197
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3 KDF	#161, #386, #388
Deterministic Random Bit Generator (DRBG)	SP800-90A CTR_DRBG; Hash_Based DRBG	#442
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#819 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.

Algorithm	Supports	Certificate
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1679
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approved mode of operation.	1024-bit and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approved mode of operation.	#1396 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approved mode of operation.
Secure Hash Algorithm (SHA)	SHA-1, SHA-256, SHA-384, and SHA-512	#2265
SP800-108 KDF	KBKDF	#36
Triple Data Encryption Algorithm (Triple-DES) NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	KO 1 ECB and CBC mode NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	#1617 NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.

Table 29 - Algorithm Certificates for the ICX 6610 Devices

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Following table, below, lists all algorithm certificates for the ICX 7450 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that “IS NOT” available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that “ARE NOT” available within any service in the Approved mode of operation.	ECB, CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that “IS NOT” available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that “ARE NOT” available within any service in the Approved mode of operation.	#2981, #3142 NOTE: AES 192 is latent functionality that “IS NOT” available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that “ARE NOT” available within any service in the Approved mode of operation.
AES-CMAC	AES-CMAC	#3438
AES Key Wrap	AES-KW	#3438
AES GCM	GCM	#1269
AES	ECB (128 bits)	#1269
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3 KDF	#362, #390, #400
Deterministic Random Bit Generator (DRBG)	SP800-90A CTR_DRBG; Hash_Based DRBG	#569
Digital Signature Algorithm (DSA) NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	#887 NOTE: Latent functionality ”IS NOT” available within any service in the Approved mode of operation
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1and HMAC SHA-256	#1890

Algorithm	Supports	Certificate
Rivest Shamir Adleman Signature (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approve mode of operation.	1024 and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approve mode of operation.	#1565 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and “IS NOT” available within any service in the Approve mode of operation.
Secure Hash Algorithm (SHA)	SHA-1, SHA-256, SHA-384, and SHA- 512	#2505
SP800-108 KDF	KBKDF	#58
Triple Data Encryption Algorithm (Triple-DES) NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	KO 1 ECB and CBC mode NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.	#1764 NOTE: Latent functionality “IS NOT” available within any service in the Approved mode of operation.

Table 30 - Algorithm Certificates for the ICX 7450 Devices

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.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

The following table provides information about RSA certificate usage. Each of the listed CSPs/Keys and algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware.

For details on protocols used with these certificates please see section 14, Appendix B: Critical Security Parameters.

CSPs/Keys	ICX 6610	ICX 7450
Firmware Integrity / Firmware Load RSA Public Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
SSHv2 Client RSA Public Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
SSHv2 Host RSA Private Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
SSHv2 Host RSA Public Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
TLS Host Public Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
TLS Host RSA Private Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)
TLS Peer Public Key	#1396 (2048 bit SHA256)	#1565 (2048 bit SHA256)

Table 31 – *RSA Algorithm Certificates usage*

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.2 Displaying Mode Status

Brocade cryptographic modules provide the *fips show* command to display status information about the device's FIPS mode. This command displays information about the policy settings. 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 10.1, FIPS Approved Mode.

The following example shows the output of the *fips show* command before an operator enters the *fips enable* command. Displayed status information indicates that 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. Displayed status information indicates that 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).

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be fips
compliant and has to be zeroized. The system needs to be reloaded to operate
in FIPS mode.
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords: Clear
SSHv2 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. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) and the device is enforcing a security policy (Operational Status is ON).

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:    Clear
SSHv2 RSA Host Keys: Clear
HTTPS RSA Host Keys and Signature:     Clear
```

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.3 Invoking FIPS Approved Mode

Crypto Officer may use “FastIron FIPS and Common Criteria Configuration Guide” documentation on myBrocade.com for configuration of these 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 used by various networking protocols including host access passwords, SSHv2 host keys, and HTTPS host keys with the digital signature.

4) Enter command: *`no web-management hp-top-tools`*

   The device will turn off access by HP ProCurve Manager via port 280.

5) Generate the SSHv2 Host RSA Private Key (2048 bit) and SSHv2 Host RSA Public Key.
   a) Use CLI command: *`crypto key generate`*
6) Generate the TLS Host RSA Private Key (RSA 2048 bit) and TLS Host Public Key (RSA 2048 bit).
   a) Use CLI command: *`crypto-ssl certificate generate`*

   NOTE: The command syntax above includes the nomenclature "ssl" from a legacy command line API; for the avoidance of doubt it is hereby stated that such syntax is a misnomer as SSL "IS NOT" supported in FIPS mode (i.e. the cryptographic module enforces the use of TLS in FIPS mode; SSL "IS NOT" supported in FIPS mode)

7) Copy signature files of all the affected images to the flash memory.
   a) Use CLI command: *`scp <syntax>`*
8) Enter command: *`write memory`*.

   The device saves the running configuration as the startup configuration.

9) Enter command: *`reload`*

   The device resets and begins operation in FIPS Approved mode.
   (**NOTE**: Do not press B as the module is reloading).

10) Enter command: *`fips show`* (This command displays the FIPS-related status, which should confirm the security policy is the default security policy.)

11) Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

11 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
GCM	Galois/Counter Mode symmetric key cryptographic
GMAC	Galois Message Authentication Code (GMAC): an authentication-only variant of the GCM
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
MACsec	MAC Security standard
Mbps	Megabits per second
NDRNG	Non-Deterministic Random Number Generator
POE	Power over Ethernet
POE+	High Power over Ethernet
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell
TACACS+	Terminal Access Control Access-Control System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

Table 32 - Glossary

12 References

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

[FIPS 186-4] Digital Signature Standard (DSS), July 2013

[RSA PKCS #1] PKCS #1: RSA Cryptography Specifications Version 2.1

[SP800-90A Rev.1] National Institute of Standards and Technology Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13 Appendix A: Tamper Evident Label application

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

1) Tamper evident label security seals
    a) Count 120
    b) Checkerboard destruct pattern with ultraviolet visible “Secure” image

Use 99% isopropyl or ethyl alcohols to clean the surface area at each tamper evident label security seal placement location. Cleaning alcohol is not provided in the kit. However, cleaning 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 Crypto Officer is responsible for securing and having control of any unused seals at all times.

Tamper evidence information

When a tamper evident label security seal is removed from the surface to which it has been applied, several tamper indications are apparent:

- The seal that has been removed shows a checkerboard destruct pattern.
- The graphics printed within the seal are uniquely split between the removed seal and the residue left on the surface. The residue is visible under ultraviolet light.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1 ICX 6610 devices

13.1.1 ICX6610-24F Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6610-24F devices. Each device requires the placement of eighteen (18) seals:

- **Front:** Affix one (1) seal 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 52 and Figure 53 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 53 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 of the seal is affixed to the side of the device and the other 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 53 for correct seal orientation and positioning on the side of the device.

Figure below illustrates front view of a Brocade ICX6610-24F device with security seals

Figure 52 - ICX6610-24F - Front view with tamper evident label security seals

Next page →

Figure below illustrates top, front, and left side view of a Brocade ICX 6610-24F device with security seals

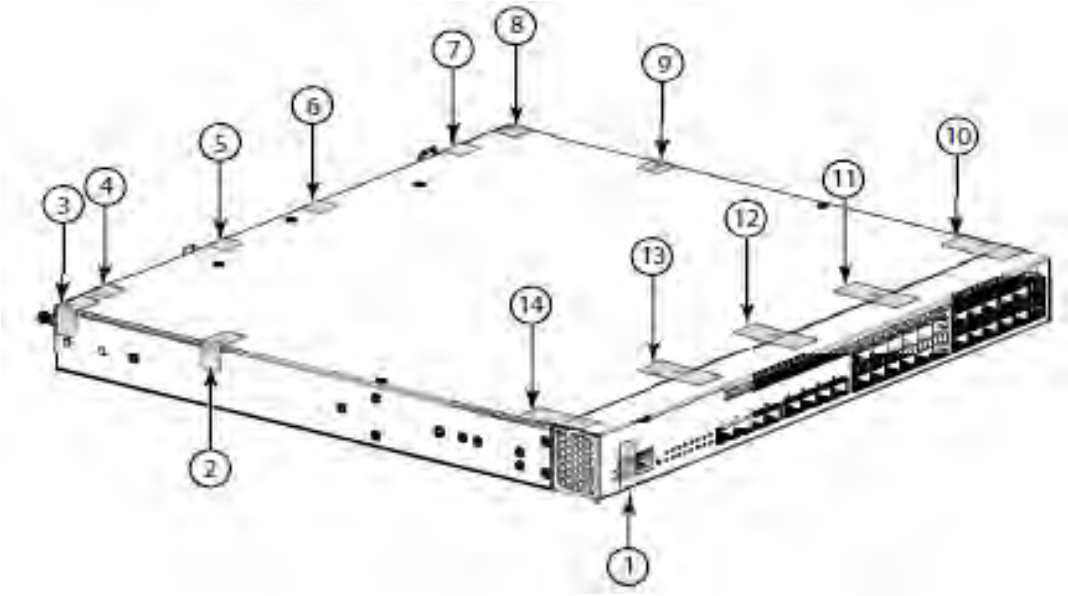

Figure 53 - ICX6610-24F - Top, front and left side view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- 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 of the seal is affixed to the rear panel of the device and the other part is affixed to the top cover or chassis bottom. Refer to Figure 54 for correct seal orientation and positioning.

Note the placement of the seal (15) below the power supply handle.

Figure below illustrates rear view of a Brocade ICX6610-24F device with security seals

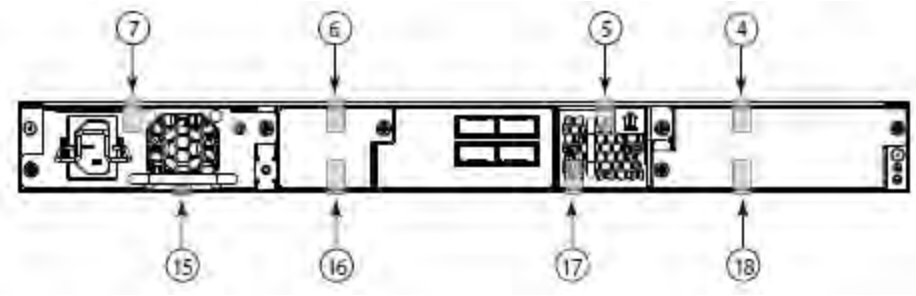

Figure 54 - ICX6610-24F - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1.2 ICX6610-24 and ICX6610-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6610-24 and ICX6610-24P devices. Each device requires the placement of eighteen (18) 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 55 and Figure 56 for correct seal orientation and positioning.
- **Top:** Affix five seals (5) 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 56 for correct seal orientation and positioning.
- **Right and left sides:** Affix two seals (2) to each side of the device. Place the seals in a 90 degree bend, so that part of the seal is affixed to the side of the device and the other 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 56 for correct seal orientation and positioning on the side of the device.

Figure below illustrates front view of Brocade ICX6610-24 and ICX6610-24P devices with security seals

Figure 55 - ICX6610-24 and ICX6610-24P - Front view with tamper evident label security seals

Next page →

Figure below illustrates front, top, and left side view of Brocade ICX6610-24 and ICX6610-24P devices with security seals

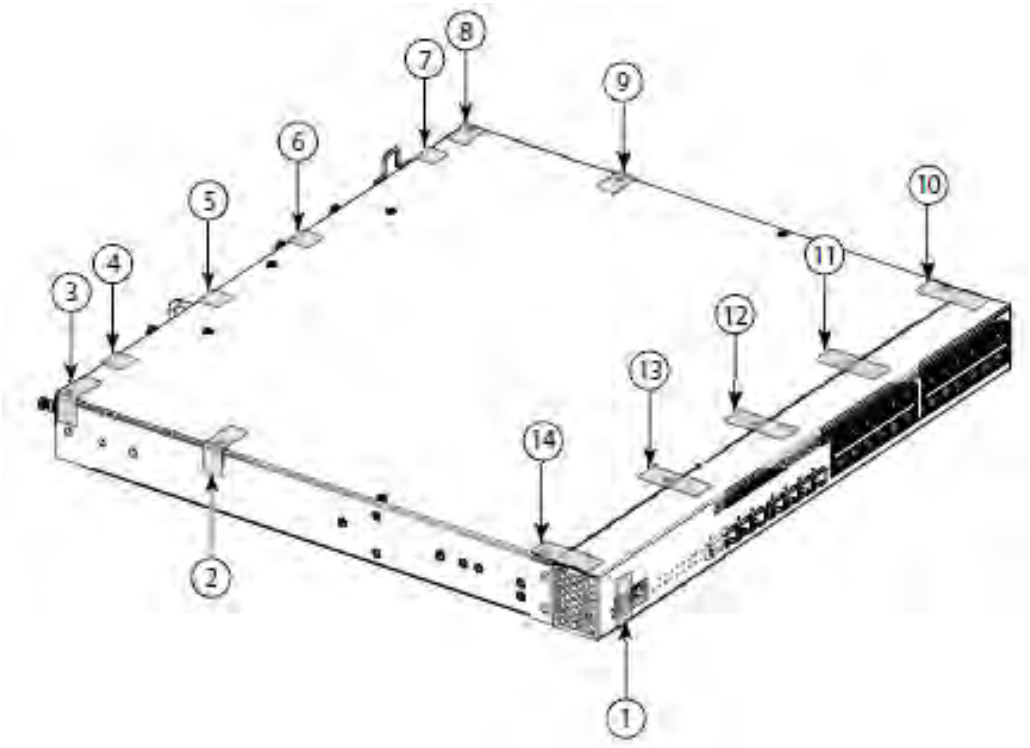

Figure 56 - ICX6610-24 and ICX6610-24P - Front, top and left side view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- **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 of the seal is affixed to the rear panel of the device and the other part is affixed to the top cover or chassis bottom as shown. Refer to Figure 57 for correct seal orientation and positioning.

Note the placement of the seal (15) below the power supply handle.

Figure below illustrates rear view of Brocade ICX6610-24 and ICX6610-24P devices with security seals

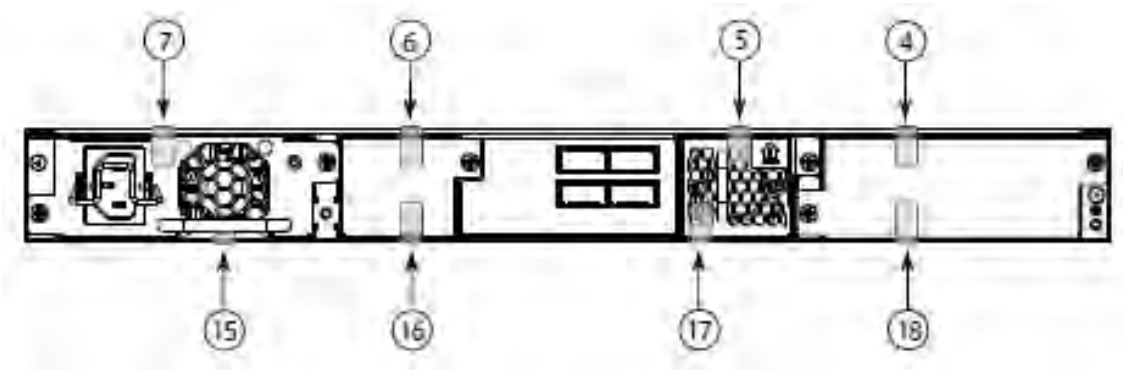

Figure 57 - ICX6610-24 and ICX6610-24P - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1.3 ICX6610-48 and ICX6610-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6610-48 and ICX6610-48P devices. Each device requires the placement of eighteen (18) 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 58 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 of the seal is affixed to the side of the device and the other 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 58 for correct seal orientation and positioning on the side of the device.

Figure below illustrates front, top, and left side view of Brocade ICX6610-48 and ICX6610-48P devices with security seals

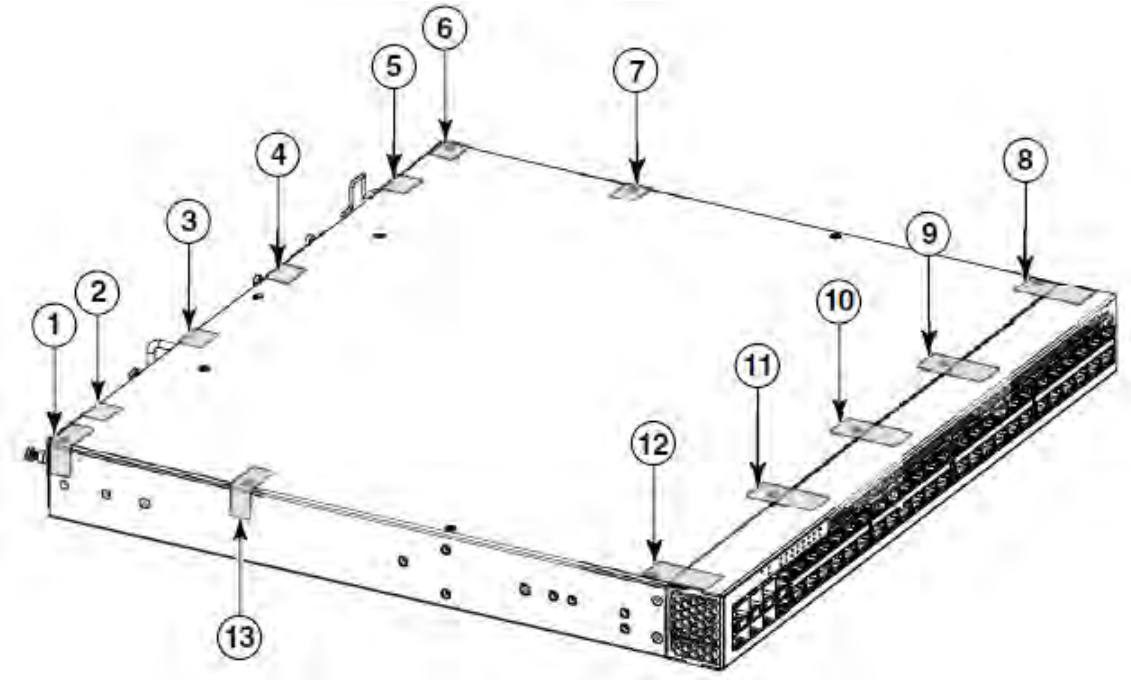

Figure 58 - ICX6610-48 and ICX6610-48P - Front, top and left side view with tamper evident label security seals

- 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 of the seal is affixed to the rear panel of the device and the other 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 59 for correct seal orientation and positioning.

Note the placement of the seal (14) below the power supply handle.

Figure below illustrates rear view of Brocade ICX6610-48 and ICX6610-48P devices with security seals

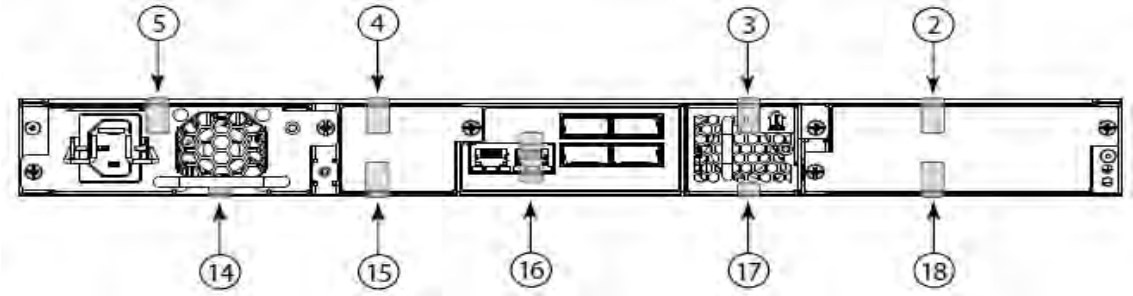

Figure 59 - ICX6610-48 and ICX6610-48P - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.2 ICX 7450 Devices

General guidelines:

- Figure 60 through Figure 65 display the tamper label placement on the Brocade ICX7450 (total tamper label count: 14).
- All ICX7450 models require the same total quantity of tamper labels.
- These tamper labels are to be placed in the same positions for each ICX7450 model.

Front side guidelines:

- Figure 60 and Figure 61 demonstrate the front side of a module with 24 ports, and a module with 48 ports, respectively.
- Figure 60, below, illustrates front side of the Brocade ICX 7450 with 24 ports. Quantity of 2 tamper labels are placed to cover the console port (label 14), and to secure the removable component to the module (label 10).

Figure 60 - ICX7450 with 24 ports - Front side

- Figure 61, below, illustrates the front side of the Brocade ICX7450 with 48 ports. Quantity of 2 tamper labels are placed to cover the console port (label 14), and to secure the removable component to the module (label 10).

Figure 61 - ICX7450 with 48 ports - Front side

Top side guidelines:

- Figure 62, below, illustrates top side of the Brocade ICX7450. Quantities of 11 tamper evident label seals are to be placed on the top side of the module.
- Tamper evident label seals 1, 12, 11 and 9 cover screws near the front side of the module.
- Tamper evident label seals 3, 4, 5, 6 and 7 secure the fans, removable components, and filler panel located on the rear side of the module to the top side of the module.
- Tamper evident label seal 2 and tamper evident label seal 8 secure the top cover to the left and right sides, respectively, of the module.

Figure 62 - ICX7450 - Top side

Next page →

Rear side guidelines:

- Figure 63, below, illustrates rear side of the Brocade ICX7450. In addition to tamper evident label seals 3, 4, 5, 6 and 7 that is described in Figure 63, quantity of one tamper label seal is utilized to secure the power supply to the bottom of the module (label 13).

Figure 63 - ICX7450 - Rear side

Left and right side guidelines:

- Figure 64, below, illustrates left side of the Brocade ICX7450. Quantity of one tamper evident label seal is placed on the left side (label 2), and secures the top covers to the left side of the module.

Figure 64 - ICX7450 - Left side

- Figure 65, below, illustrates right side of the module Brocade ICX7450. Quantity of one tamper evident label seal is placed on the right side (label 8), and secures the top cover to the right side of the module.

Figure 65 - ICX7450 - Right side

14 Appendix B: Critical Security Parameters

The module supports the following CSPs and public keys:
1) SSHv2 Host RSA Private Key (2048 bit)
- Description: Used to authenticate SSHv2 server to client
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: N/A
- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

2) SSHv2 DH Private Key (2048 bit)
- Description: Used in SCP and SSHv2 to establish a shared secret
- Type: DH Private Key
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Session termination and "fips zeroize all" command

3) SSHv2 DH Shared Secret Key (2048 bit)
- Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- Type: DH Shared Secret Key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

4) SSHv2/SCP Session Keys (128 and 256 bit AES CBC)
- Description: AES encryption key used to secure SSHv2/SCP
- Type: AES CBC Key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A

- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

5) SSHv2/SCP Authentication Key (160 bits HMAC-SHA-1)
- Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
- Type: HMAC-SHA-1
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

6) SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Type: KDF
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

7) TLS Host RSA Private Key (RSA 2048 bit)
- Description: RSA key used to establish TLS v1.0/1.1 and v1.2 sessions
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: N/A
- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

8) TLS Pre-Master Secret
- Description: Secret value used to establish the Session and Authentication key
- Type: TLS v1.0/1.1 and v1.2 CSP
- Generation: N/A, established during the TLS v1.0/1.1 and v1.2 handshake using RSA key transport
- Establishment: Key transport: RSA key wrapped over TLS v1.0/1.1 and v1.2 session; allowed as per FIPS 140-2 IG D.9.

- Entry: Key transport: RSA key wrapped over TLS v1.0/1.1 and v1.2 session; allowed as per FIPS 140-2 IG D.9.
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

9) TLS Master Secret
- Description: 48 bytes secret value used to establish the TLS v1.0/1.1 and v1.2 Session Key and TLS Authentication Key
- Type: TLS v1.0/1.1 and v1.2 CSP
- Generation: N/A
- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

10) TLS KDF Internal State
- Description: Values of the KDF internal state
- Type: TLS v1.0/1.1 (HMAC-SHA-1, HMAC-MD5) as per SP800-135 and TLS v1.2 (HMAC-SHA-256) as per SP800-135
- Generation: Approved TLS v1.0/1.1 and v1.2 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

11) TLS Session Key
- Description: 128 or 256 bit AES CBC key used to secure TLS v1.0/1.1 and v1.2 sessions
- Type: AES CBC
- Generation: N/A
- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

12) TLS Authentication Key
- Description: HMAC-SHA-1 key used to provide data authentication for TLS v1.0/1.1 sessions; HMAC-SHA-1 and HMAC-SHA-256 keys used to provide data authentication for TLS v1.2
- Type: TLS v1.0/1.1 (HMAC-SHA-1) and TLS v1.2 (HMAC-SHA-1 and HMAC-SHA-256)

- Generation: N/A
- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

13) DRBG Seed
- Description: Seeding material for the SP800-90A CTR_DRBG
- Type: DRBG Seed material
- Generation: internally generated; raw random data from NDRNG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Session termination and "fips zeroize all" command

14) DRBG Value V
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

15) DRBG Key
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

16) DRBG Internal State
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A

- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

17) User Password
- Description: Password used to authenticate User (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

18) Port Administrator Password
- Description: Password used to authenticate Port Configuration Administrator (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

19) Crypto Officer Password
- Description: Password used to authenticate Crypto Officer (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

20) RADIUS Secret
- Description: Used to authenticate the RADIUS server (8 to 64 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: Plaintext in RAM, Brocade proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash
- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

21) TACACS+ Secret
- Description: Used to authenticate the TACACS+ server (8 to 64 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: Plaintext in RAM, Brocade proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

22) Firmware Integrity / Firmware Load RSA Public Key
- Description: RSA 2048-bit public key used to verify signature of firmware of the module
- Type: RSA Public Key
- Generation: N/A, Generated outside the module
- Establishment: N/A
- Entry: Through firmware update
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

23) SSHv2 Host RSA Public Key
- Description: (2048 bit); Used to establish shared secrets
- Type: RSA Public Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

24) SSHv2 Client RSA Public Key
- Description: (2048 bit); Used to establish shared secrets
- Type: RSA Public Key
- Generation: N/A, generated outside the module
- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

25) SSHv2 DH Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
- Type: DH Public Key
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

26) SSHv2 DH Peer Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
- Type: DH Peer Public Key
- Generation: N/A
- Establishment: N/A
- Entry: Plaintext
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process

27) TLS Host Public Key (RSA 2048 bit)
- Description: Used by client to encrypt TLS Pre-Master secret
- Type: TLS host Public key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

28) TLS Peer Public Key (RSA 2048 bit)
- Description: Used to authenticate the client
- Type: TLS Peer Public Key
- Generation: N/A
- Establishment: N/A
- Entry: Plaintext during TLS v1.0/1.1 and v1.2 handshake protocol
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

29) SNMPv3 secret
- Description: Used for authentication (SHA1, Password is 8 to 16 characters long) and for privacy (AES-CFB 128-bit, Password 12 to 20 characters)
- Type: Authentication data and privacy
- Generation: N/A - generated outside of the module

- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
- Storage: SHA1 digest and AES are stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

30) NTP secret
- Description: Authentication (SHA1, Password is 8 to 16 characters long)
- Type: Authentication data
- Generation: N/A - generated outside of the module
- Establishment: N/A
- Entry: Configured by the operator, entered authenticated over SSHv2 session
- Output: SHA1 hashed in configuration, output authenticated over SSHv2 session
- Storage: SHA1 digest is stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

31) CAK
- Description: Connectivity association key - main master key; Pre-shared key; 128 bits in length
- Type: KDF Input
- Generation: N/A - generated outside of the module
- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Storage: Plaintext in configuration file (Flash); Save configuration
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

32) CKN
- Description: Connectivity key name; pre-shared key; 128 bits in length)
- Type: KDF input
- Generation: N/A - generated outside of the module
- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Storage: Plaintext in configuration file (Flash); Save configuration
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

33) ICK
- Description: Integrity checksum key; 128 bits

- Type: AES CMAC 128
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

34) KEK
- Description: Key encryption key; 128 bits
- Type: AES Key Wrap
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

35) SAK
- Description: Secure association key; 128 bits
- Type: GCM Key
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: Key transport: AES Encrypted with the KEK; Allowed as per FIPS 140-2 IG D.9
- Entry: Input AES encrypted by the KEK
- Output: Output AES encrypted by the KEK
- Storage: Plaintext in RAM and Plaintext in Marvell chip
- Key-to-Entity: Process: MACsec
- Zeroization: Session termination and "fips zeroize all" command

36) SP800-108 KDF Internal State
- Description: SP800-108 KDF
- Type: SP800-108 (AES 128 CMAC in Counter Mode)
- Generation: SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command