HP Virtual Connect 16Gb 24-Port FC Module

FIPS 140-2
Non-Proprietary Security Policy

Document Version 1.0

Hewlett-Packard Company

September 28, 2014

Document History

Version	Summary of Changes	Publication Date
1.0	Initial Release	December 1, 2014

1 Module Overview

The HP Virtual Connect 16Gb 24-port FC Module, hereby referred to as the “module”, is a multi-chip embedded module that meets FIPS 140-2 Level 1 security requirements. The cryptographic module will be embedded inside HP BladeSystem c-Class enclosures (Host equipment outside of the physical cryptographic boundary of the cryptographic module). The module’s cryptographic boundary is defined as the outside physical perimeter that is displayed in Figures 1 – 6, which is placed inside HP BladeSystem c-Class enclosures.

HP Virtual Connect is a set of interconnect modules and embedded software for HP BladeSystem c-Class Enclosures host equipment outside of the cryptographic boundary. The Virtual Connect Module (VCM) is software embedded on VC-Enet modules outside of the physical cryptographic boundary used to manage the cryptographic module’s customizable mapping of external ports with internal ports.

Firmware Version	VC 4.40
Hardware Version	40-1000779-08 Rev C
Hardware Part Number	80-1007799-04

Table 1 Module Firmware and Hardware Version

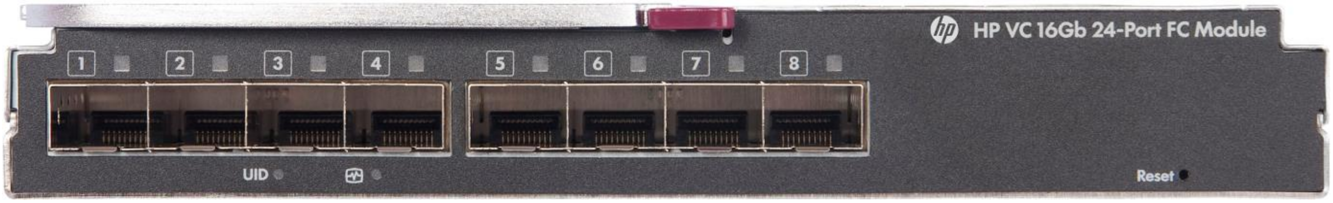

Figure 1 Front side of HP Virtual Connect 16Gb 24-port FC Module

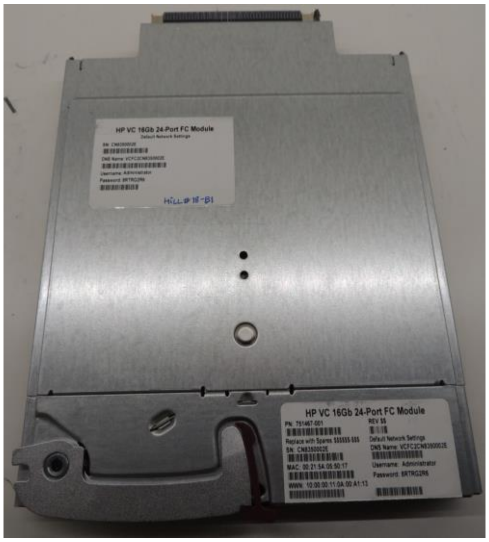

Figure 2 Top side of HP Virtual Connect 16Gb 24-port FC Module

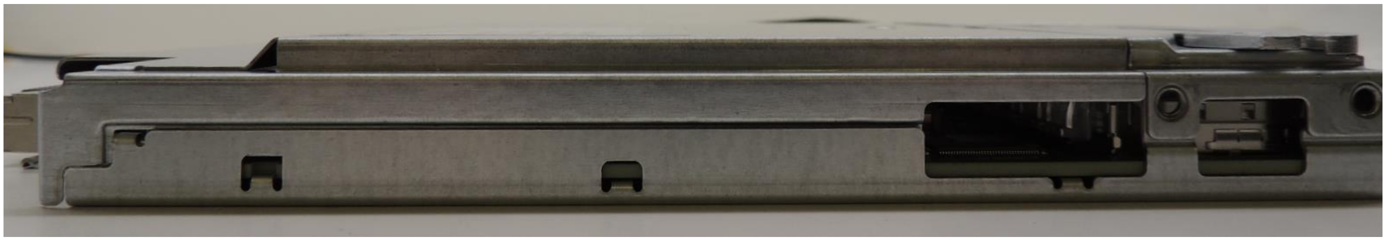

Figure 3 Left side of HP Virtual Connect 16Gb 24-port FC Module

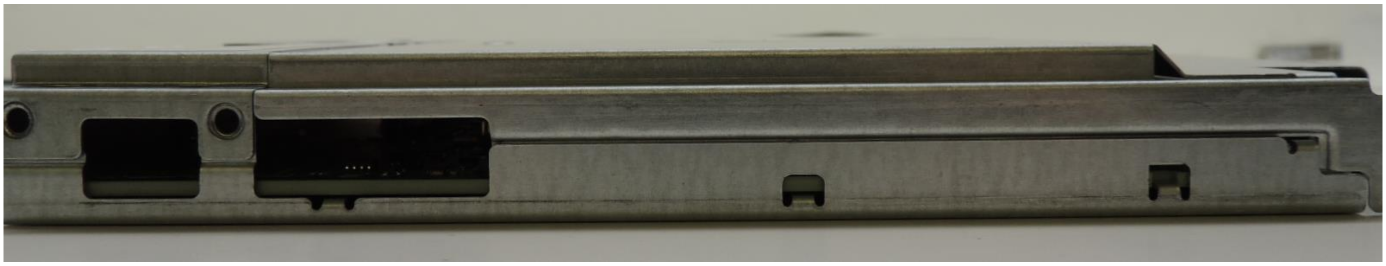

Figure 4 Right side of HP Virtual Connect 16Gb 24-port FC Module

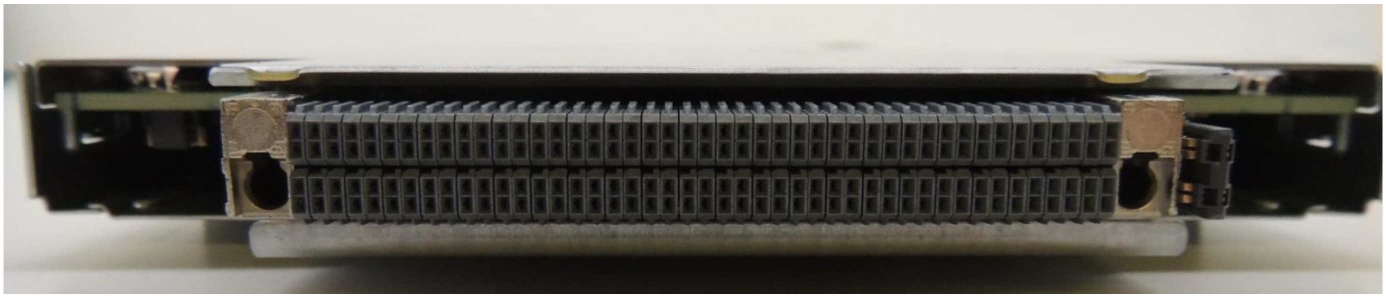

Figure 5 Back side of HP Virtual Connect 16Gb 24-port FC Module

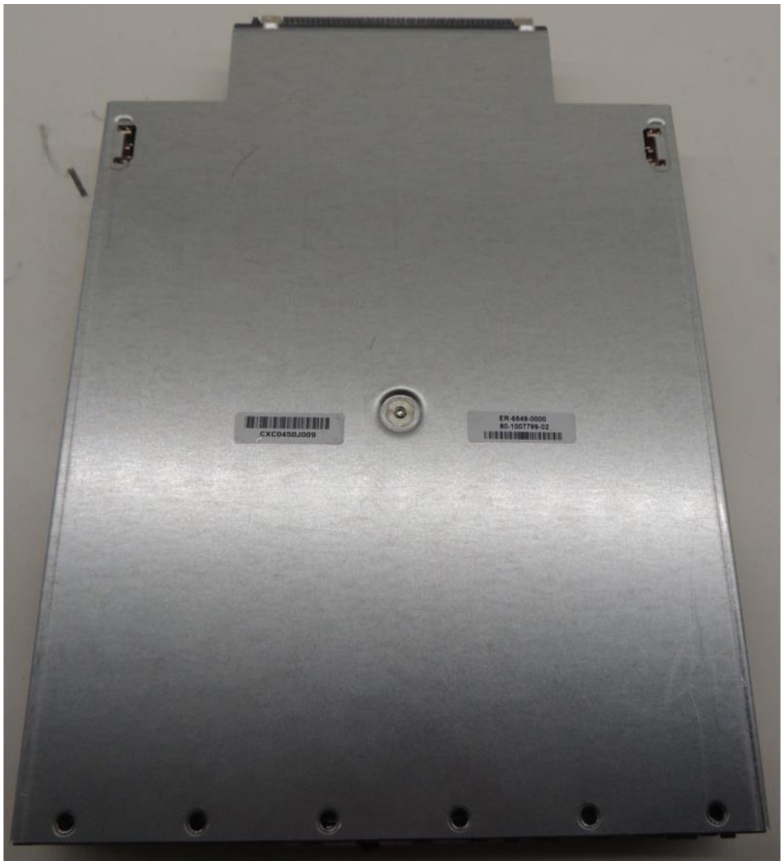

Figure 6 Bottom side of HP Virtual Connect 16Gb 24-port FC Module

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 2 Module Security Level Specification

3 Modes of Operation

3.1 Approved mode of operation

The cryptographic module supports the following Approved algorithms:

Approved Algorithm	Certificate Number	Implementation
AES	1596	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
HMAC-SHA-256	934	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
HMAC-SHA-512	934	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
HMAC-SHA-1	934	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
RNG	1252	Brocade FIPS Crypto Library; Version v7.2.0 (Firmware)
RSA	1389	Brocade FIPS Crypto Library; Version v7.2.0 (Firmware)
SHS [SHA-1]	1408	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
SHS [SHA-256]	1408	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
SHS [SHA-512]	1408	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
Triple-DES	1043	Brocade FIPS Crypto Library (AMCC); Version OpenSSL V1.0 (Firmware)
CVL	157, 363	Brocade FIPS Crypto Library; Version v7.2.0 (Firmware) Brocade FIPS Crypto Library; Version v7.2.1_hil (Firmware)
ECDSA	548	Brocade FIPS Crypto Library; Version v7.2.1_hil (Firmware)

Table 3 Approved Algorithms available in firmware

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

The following non-Approved algorithms and protocols are allowed within the Approved mode of operation:

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)

- MD5 (used for password hash. Note: The use of MD5 does not provide cryptographic protection, and is considered as plaintext.)

- Non-deterministic random number generator for seeding ANSI X9.31 DRNG

The initial state of the cryptographic module is in a non-FIPS Approved mode of operation. The cryptographic module contains a default “root” account that has a unique password set in factory. The root account is disabled once the cryptographic module is set to FIPS Approved mode of operation by the Crypto-Officer.

The cryptographic module may be configured for the FIPS approved mode of operation by the Crypto Officer by following the procedure:

1. Verify the interconnect module firmware is 4.40 for all modules in the c-Class enclosure. If the firmware version is not 4.40, upgrade the firmware to 4.40.

2. Remove the Virtual Connect Ethernet module hosting Virtual Connect Manager module from the interconnect bay.

3. Remove the access panel.

Removing the access panel is not required on HP VC FlexFabric-20/40 F8 modules. The DIP switch is accessible without removing the access panel.

4. Locate the DIP switch as described in the HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide.

5. Find DIP switch 3, and then set to the ON position. Be sure that all other switches remain in the OFF position.

OFF OFF ON OFF

6. Install the access panel.

7. Install the Virtual Connect Ethernet module into the interconnect bay and allow the module to power up and reach a fully booted and operational state (approximately 1 minute).

8. Log in to VC Manager and verify the domain and interconnect modules are in FIPS mode.

3.2 Non-FIPS Approved mode of operation

The cryptographic module's initial state is in a non-FIPS Approved mode of operation. In the non-FIPS Approved mode, an operator will have no access to CSPs used within the FIPS Approved mode of operation. The Crypto-Officer is required to follow the procedures in the Security Policy to properly enable the FIPS Approved mode of operation. Once the cryptographic module is in the FIPS Approved mode of operation, it cannot exit this mode. Any attempt by the operator to exit the FIPS Approved mode of operation is a strict violation of the Security Policy and deems the cryptographic module fully non-compliant and unfit for service to protect sensitive unclassified data with cryptography.

The following cipher suites are allowed in non-FIPS Approved mode for configuring SSL and TLS:

aes-128-cbc,3des-cbc,aes-256-cbc

The following message digests functions are allowed in non-FIPS Approved mode:

hmac-md5, hmac-sha-1, hmac-sha-256

The following message authentication algorithms and ciphers are allowed in non-FIPS Approved mode for configuring SSH:

Ciphers:

aes-128-ctr,aes-192-ctr,aes-256-ctr,aes-128-gcm,aes-192-gcm,aes-256-gcm,aes-128-cbc,3des-cbc,aes-192-cbc,aes-256-cbc

Macs: hmac-md5,hmac-sha-1,hmac-sha-256,hmac-sha-512

The following is only allowed in non-FIPS Approved mode of operation:

- SNMPv3 KDF (non-compliant)

4 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

A). Faceplate connections:

- 8 Fibre Channel connections (SFP+) capable of supporting 4Gb, 8Gb and 16Gb FC speeds: Data Input, Data Output, Control Input, Status Output
- LEDs: Status output (18)

B). Backplane connections:

- Bay Presence: Status Output
- Bay ID Pins (x3): Status Output
- I^{2}C : Data Input, Data Output
- Serial R232 Management Port: Data Input, Data Output, Control Input, Status Output
- 100Mb Ethernet management Port: Data Input, Data Output, Control Input, Status Output
- 8 Gb/16Gb Fibre channel Serial Connections: Data Input, Data Output, Control Input, Status Output
- Power connection: Power

4.1 LED Indicators

The cryptographic module contains the following LEDs:

a) Port ID LED (for each SFP+ connector)
b) Port Status and Link/Activity LED (for each SFP+ connector)
c) UID LED
d) Health LED

Color	Function
Unlit	Port has not been configured
Green	Port is configured as an uplink port

Table 4 Port ID LED Definitions

Color	Function
Unlit	No power or signal on the port
Green - Steady	Port is online, but not passing traffic
Green - Flickering	Port is online, passing traffic
Amber – Steady	Port has light or signal, but not yet online
Amber – Slow Flashing	Port is disabled
Amber – Fast flashing	Port is faulty or invalid SFP

Table 5 Port Status and Link/activity LED Definitions

Color	Function
Unlit	UID is OFF
Blue - Steady	UID is ON

Table 6 UID LED Definitions

Color	Function
Unlit	Switch is OFF
Green – Steady	Switch is ON and functioning; no fault

Table 7 Health LED Definitions

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports a Crypto-Officer role and a User role. The operator implicitly assumes a role by using the Virtual Connect Module (software embedded on VC-Enet modules outside of the physical cryptographic boundary) to invoke services that are associated with each role. Table 6 contains services available for operators, and it provides a brief description regarding the service functions.

Service Name	Description
FIPSCfg	Control FIPS mode operation and related functions
Zeroize	Zeroize all CSPs
Firmware Management	Control firmware management

Table 8 Service Descriptions

6 Access Control Policy

6.1 Roles and Services

Table 7 contains the services authorized for each role. Boxes marked with an “X” refer to the role authorized to access the corresponding service.

	User	Crypto-Officer
FIPSCfg		X
Zeroize		X
Firmware Management	X	X

Table 9 Services Authorized for Roles

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

6.3 Definition of Critical Security Parameters (CSPs)

- DH Private Keys for use with 2048 bit modulus in SSHv2
- SSH/SCP/SFTP Session Keys – 128, 192 and 256 bit AES CBC, Three Key TDES
- SSH/SCP/SFTP Authentication Key - HMAC-SHA-1 (160 bits), HMAC-SHA-256, HMAC-SHA-512
- SSH KDF Internal State
- SSH DH Shared Secret Key (2048 bits)
- SSH EC-DH Shared Secret Key (256 bits)
- SSH RSA 2048 bit Private Key
- SSH ECDSA 256 bit Private Key
- Value of K during SSH 256 ECDSA session
- TLS Private Key (RSA 2048)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS PRF Internal State
- TLS Session Keys – 128, 256 bit AES CBC, Three Key TDES CBC
- TLS Authentication Key for HMAC-SHA-1 (160 bits), HMAC-SHA256 and HMAC-SHA-384
- Approved RNG Seed Material
- ANSI X9.31 DRNG Internal State
- Passwords

6.4 Definition of Public Keys:

The following are the public keys contained in the module:

- SSH DH Public Key (2048 bit modulus)
- SSH DH Peer Public Key (2048 bit modulus)
- TLS v1.0/TLS v1.2 Public Key (RSA 2048)
- TLS v1.0/ TLS v1.2 Peer Public Key (RSA 2048)
- Firmware Download Public Key (RSA 2048 SHA-256)
- SSH RSA 2048 bit Public Key
- SSH RSA 2048 bit Host Public Key
- SSH ECDSA 256 bit Host Public Key

6.5 Definition of CSPs Modes of Access

Table 6 CSP Access Rights within Roles & Services defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- R: Read
- W: Write
- N: No Access
- Z: Zeroize (zeroization is performed by the operator via the VCM)

Services	Crypto-Officer	Crypto-Officer	Crypto-Officer & User
CSPs	FIPSCFg	Zeroize	FirmwareManagement
DH Private Keys for use with 2048 bit modulus in SSHv2	RW	Z	N
SSH/SCP/SFTP Session Keys – 128, 192 and 256 bit AES CBC, Three Key TDES	RW	Z	N
SSH/SCP/SFTP Authentication Key	RW	Z	N
SSH KDF Internal State	RW	Z	N
SSH DH Shared Secret Key (2048 bits)	RW	Z	N
SSH EC-DH Shared Secret Key (256 bits)	RW	Z	N
SSH RSA 2048 bit Private key	RW	Z	R
SSH ECDSA 256 bit Private Key	RW	Z	N
Value of K during SSH 256 ECDSA session	RW	Z	N
TLS Private Key (RSA 2048)	RW	Z	N
TLS Pre-Master Secret	RW	Z	N
TLS Master Secret	RW	Z	N
TLS PRF Internal State	RW	Z	N
TLS Session Keys – 128, 256 bit AES CBC, Three Key TDES CBC	RW	Z	N
TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384	RW	Z	N
Approved RNG Seed material	RW	Z	N
ANSI X9.31 DRNG Internal State	N	Z	N
Passwords	RW	Z	R

Table 10 CSP Access Rights within Roles & Services

Services	Crypto-Officer	Crypto-Officer	Crypto-Officer & User
CSPs	FIPSCFg	Zeroize	FirmwareManagement
SSH DH Public Key (2048 bit modulus)	RW	Z	R
SSH DH Peer Public Key (2048 bit modulus)	RW	Z	N
TLS v1.0/TLS v1.2 Public Key (RSA 2048)	RW	Z	N
TLS v1.0/ TLS v1.2 Peer Public Key (RSA 2048)	RW	Z	N
Firmware Download Public Key (RSA 2048 SHA-256)	N	Z	RW
SSH RSA 2048 bit Public Key	RW	Z	R
SSH RSA 2048 bit Host Public Key	RW	Z	R
SSH ECDSA 256 bit Host Public Key	RW	Z	R

Table 11 Public Key Access Rights within Roles & Services

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code signed by RSA 2048 with SHA-256 may be executed.

8 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS140-2 Level 1 module.

1) The cryptographic module shall perform the following tests:

    a) Power up Self-Tests:

    i) Cryptographic algorithm tests:

    (1) Three Key TDES CBC KAT (encrypt)
    (2) Three Key TDES CBC KAT (decrypt)
    (3) AES (128, 192, 256) CBC KAT (encrypt)
    (4) AES (128, 192, 256) CBC KAT (decrypt)
    (5) HMAC-SHA-1 KAT
    (6) HMAC-SHA-256 KAT
    (7) HMAC-SHA-512 KAT
    (8) ANSI X9.31 DRNG KAT
    (9) SHA-1 KAT
    (10) SHA-256 KAT
    (11) SHA-512 KAT
    (12) RSA 2048 SHA-256 KAT (sign)
    (13) RSA 2048 SHA-256 KAT (verify)
    (14) SP800-135 KDF KAT
    (15) ECDSA Pairwise Consistency Test (sign)
    (16) ECDSA Pairwise Consistency Test (verify)
    (17) ECCCDH KAT

    ii) Firmware Integrity Test (128-bit EDC)

    iii) Critical Functions Tests:

    (1) RSA 2048 KAT (encrypt)
    (2) RSA 2048 KAT (decrypt)

    b) Conditional Self-Tests:

    i) Continuous Random Number Generator (RNG) test – performed on non-approved RNG.
    ii) Continuous Random Number Generator test – performed on ANSI X9.31 DRNG.
    iii) RSA 2048 SHA-256 Pairwise Consistency Test (sign)
    iv) RSA 2048 SHA-256 Pairwise Consistency Test (verify)

v) RSA 2048 Pairwise Consistency Test (encrypt)

vi) RSA 2048 Pairwise Consistency Test (decrypt)

vii) Firmware Load Test (RSA 2048 SHA-256 Signature Verification)

viii) Bypass Test: N/A

ix) Manual Key Entry Test: N/A

2) At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test. The operator can command the module to perform the power-up self-test via reboot.

3) Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

4) Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

5) The module does not support a maintenance role or maintenance interface.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip embedded cryptographic module meets FIPS 140-2 Level 1 requirements, and includes the following physical security mechanisms:

- Production-grade components and production-grade enclosure

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

11 Definitions and Acronyms

AES	Advanced Encryption Standard
Blade	Any functional assembly that can be installed in a chassis, excluding power and fan FRUs
CBC	Cipher Block Chaining
CLI	Command Line interface
CSP	Critical Security Parameter
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
FRU	Field Replaceable Unit
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KDF	Key Derivation Function
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NTP	Network Time Protocol
PROM	Programmable read-only memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SHA	Secure Hash Algorithm
SSH	Secure Shell Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security Protocol

12 Abbreviations

16Gb	16 Gigabit
8Gb	8 Gigabit
SFP+	Small form-factor pluggable plus
LIC	License
FC	Fibre Channel
MGMT	Management