



HP Networking Switches

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Version 1.01

March 2012

Copyright Hewlett-Packard Company 2012, May be reproduced only in its original entirety [without revision].

Table of Contents

| | |
|---|-----------|
| 1 Introduction | 6 |
| 2 Overview | 6 |
| 2.1 Fixed-port L2/L2+ Managed Ethernet Switches | 6 |
| 2.1.1 HP 5120 EI Switch Series | 6 |
| 2.2 Fixed-port L3 Managed Ethernet Switches | 8 |
| 2.2.1 HP 5500 EI Switch Series | 8 |
| 2.2.2 HP 5800 Switch Series | 9 |
| 2.2.3 HP 5820 Switch Series | 10 |
| 2.3 Modular Ethernet Switches | 11 |
| 2.3.1 HP 7500 Switch Series | 11 |
| 2.3.2 HP 9500 Switch Series | 15 |
| 2.3.3 HP 12500 Switch Series | 16 |
| 3 Security Appliance Validation Level | 19 |
| 4 Physical Characteristics and Security Appliance Interfaces | 20 |
| 4.1 Fixed-port L2/L2+ Managed Ethernet Switches | 20 |
| 4.1.1 HP 5120-EI Switch Series | 20 |
| 4.2 Fixed-port L3 Managed Ethernet Switches | 21 |
| 4.2.1 HP 5500-EI Switch Series | 21 |
| 4.2.2 HP 5800 Switch Series | 21 |
| 4.2.3 HP 5820 Switch Series | 21 |
| 4.3 Modular Ethernet switches | 22 |
| 4.3.1 HP 7500 Switch Series | 22 |
| 4.3.2 HP 9500 Switch Series | 23 |
| 4.3.3 HP 12500 Switch Series | 23 |
| 4.4 Physical Interfaces Mapping | 23 |
| 5 Roles, Services, and Authentication | 24 |
| 5.1 Roles | 24 |
| 5.2 Services | 24 |
| 5.3 Authentication Mechanisms | 27 |
| 6 Approved Cryptographic Algorithms | 28 |
| 7 Non-approved Cryptographic Algorithms | 29 |
| 8 Cryptographic Key Management | 29 |
| 8.1 Access Control Policy | 31 |
| 9 Self-Tests | 33 |
| 9.1 Power-On Self-Tests | 33 |
| 9.2 Conditional Self-Tests | 34 |
| 10 Delivery and Operation | 34 |
| 10.1 Secure Delivery | 34 |
| 10.2 Secure Operation | 35 |
| 11 Physical Security Mechanism | 35 |
| 12 Mitigation of Other Attacks | 38 |
| 13 Documentation References | 38 |
| 13.1 Obtaining documentation | 38 |

FIPS 140-2 Non-Proprietary Security Policy for the HP Networking Switches

Keywords: Security Policy, CSP, Roles, Service, Cryptographic Module

List of abbreviations:

| Abbreviation | Full spelling |
|--------------|--|
| AAA | Authentication, Authorization, and Accounting |
| AES | Advanced Encryption Standard |
| CF | Compact Flash |
| CLI | Command Line Interface |
| CMVP | Cryptographic Module Validation Program |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DOA | Dead on arrival |
| FCoE | Fibre Channel over Ethernet |
| FIPS | Federal Information Processing Standard |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hyper Text Transfer Protocol |
| IRF | Intelligent Resilient Framework |
| KAT | Known Answer Test |
| LED | Light Emitting Diode |
| LPU | Line Processing Unit |
| MAC | Message Authentication Code |
| MAN | Metropolitan Area Network |
| MPU | Main Processing Unit |
| NIST | National Institute of Standards and Technology |
| OAA | Open Application Architecture |
| OAP | Open Application Platform |
| PSU | Power Supply Unit |
| RADIUS | Remote Authentication Dial In User Service |
| RAM | Random Access Memory |
| RSA | Rivest Shamir and Adleman method for asymmetric encryption |
| SFP | Small Form-Factor Pluggable |
| SFP+ | Enhanced Small Form-Factor Pluggable |

| Abbreviation | Full spelling |
|--------------|--|
| SHA | Secure Hash Algorithm |
| SRPU | Switching and routing processor unit |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| XFP | 10 Gigabit Small Form-Factor Pluggable |

1 Introduction

This document is a non-proprietary Cryptographic Module Security Policy for HP Networking Ethernet switches. The series includes fixed-port L2/L2+ managed Ethernet switches (HP 5120-E1), fixed-port L3 managed Ethernet switches (HP 5500-E1, HP 5800, HP 5820), and modular Ethernet switches (HP 7500, HP 9500, HP 12500). The policy describes how the HP Networking switches meet the requirements of FIPS 140-2. This document also describes how to configure HP Networking switches in FIPS 140-2 mode. This document was prepared as part of the Level 2 FIPS 140-2 validation.

FIPS 140-2 standard details the U.S. Government requirements for cryptographic security appliances. More information about the standard and validation program is available on the NIST website at csrc.nist.gov/groups/STM/cmvp/.

This document includes the following sections:

- Overview
- Security Appliance Validation Level
- Physical Characteristics and Security Appliance Interfaces
- Roles, Services and Authentication
- FIPS Approved Algorithms
- Non-FIPS Approved Algorithms
- Cryptographic Key Management
- Self-Tests
- Delivery and Operation
- Physical Security Mechanism
- Mitigation of Other Attacks
- Obtaining Documentation and Technical Assistance

2 Overview

The HP Networking provides devices are suitable for a range of uses: at the edge of a network, connecting server clusters in a data center, in an enterprise LAN core, and in large-scale industrial networks and campus networks. The series includes fixed-port L2/L2+ managed Ethernet switch appliances, fixed-port L3 managed Ethernet switch appliances, and modular Ethernet switches. Each device is based on the Comware 5.2 platform.

2.1 Fixed-port L2/L2+ Managed Ethernet Switches

2.1.1 HP 5120 EI Switch Series

The HP 5120-EI Switch Series are Gigabit Ethernet switch appliances that support static Layer 3 routing, diversified services, and IPv6 forwarding and provide up to four 10-Gigabit Ethernet (10 Gigabit Ethernet) extended interfaces. Unique Intelligent Resilient Framework (IRF) technology creates virtual fabric by virtualizing several switches into one logical device, which increases network resilience, performance, and availability while reducing operational

complexity. These switches provide Gigabit Ethernet access and can be used at the edge of a network or to connect server clusters in data centers. High scalability provides investment protection with two expansion slots, each of which can support two-port 10 Gigabit Ethernet expansion modules. High availability, simplified management, and comprehensive security control policies are among the key features that distinguish this series.

Testing included four models in the 5120-EI series:

- HP 5120-24G EI
- HP 5120-48G EI
- HP 5120-24G-PoE+ EI
- HP 5120-48G-PoE+ EI

Figure 1 shows representatives of the series. This series requires 3 Tamper-evident labels and 2 opacity shields as shown in Figure 1.

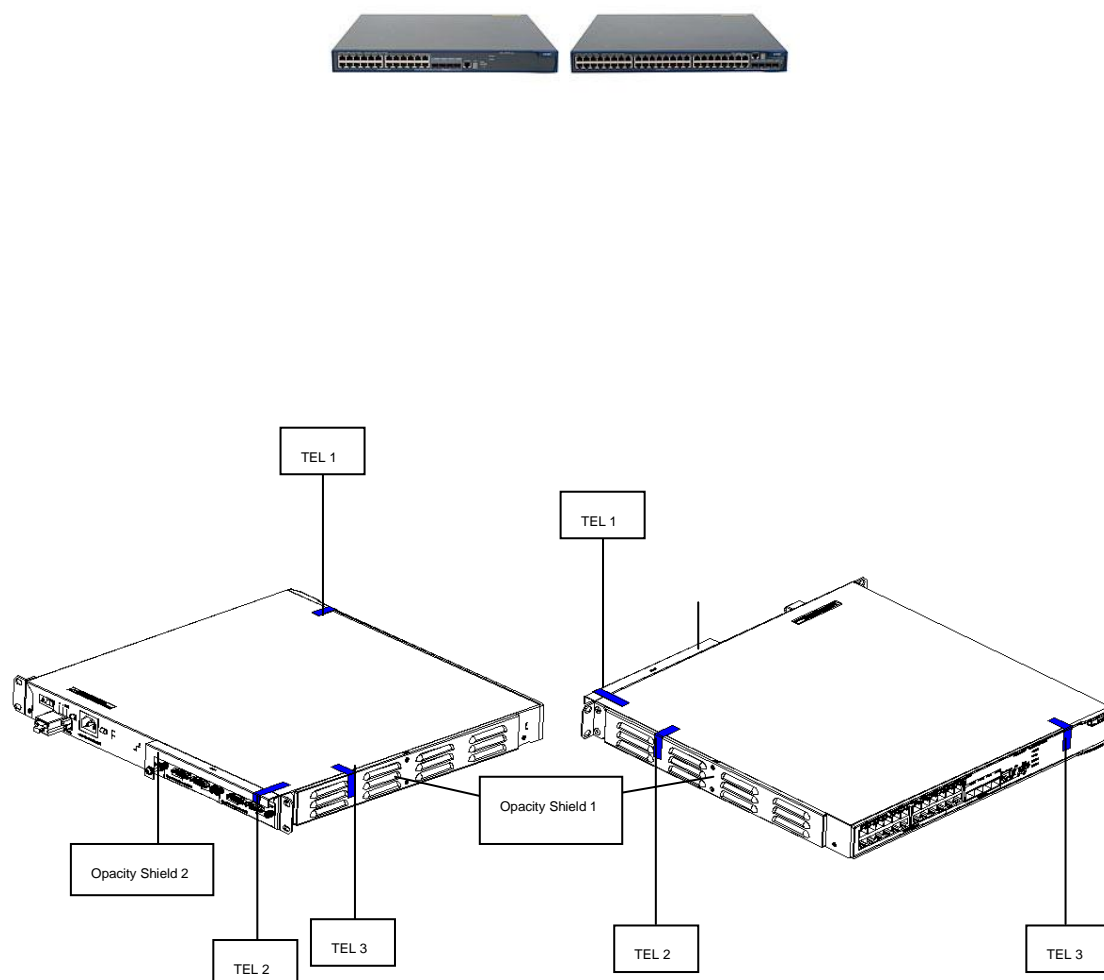


Figure 1 HP 5120-EI Switch Series Representative View

2.2 Fixed-port L3 Managed Ethernet Switches

2.2.1 HP 5500 EI Switch Series

These Gigabit Ethernet switches deliver outstanding security, reliability, and multiservice support capabilities for robust switching at the edge or aggregation layer of large enterprise and campus networks or in the core layer of SMB networks. The HP 5500 EI Switch Series is comprised of Layer 2/3 Gigabit Ethernet switches that can accommodate the most demanding applications and provide resilient and secure connectivity as well as the latest traffic prioritization technologies to enhance applications on convergent networks. With complete IPv4/IPv6 dual stack support, the series provides investment protection with an easy transition from IPv4 to IPv6 networks. Designed for increased flexibility, these switches are available with 24 or 48 Gigabit Ethernet ports. Power over Ethernet (PoE) and non-PoE models are available with optional Gigabit and 10 Gigabit Ethernet expansion capability. The all-fiber model with dual power supplies is ideal for applications that require the highest availability.

Testing included five models in the 5500 EI series:

- HP 5500-24G EI
- HP 5500-24G-PoE+ EI
- HP 5500-24G-SFP EI
- HP 5500-48G EI
- HP 5500-48G-PoE+ EI

Figure 2 shows representatives of the series. This series requires 3 Tamper-evident labels and 1 opacity shield when configured as shown in Figure 2.



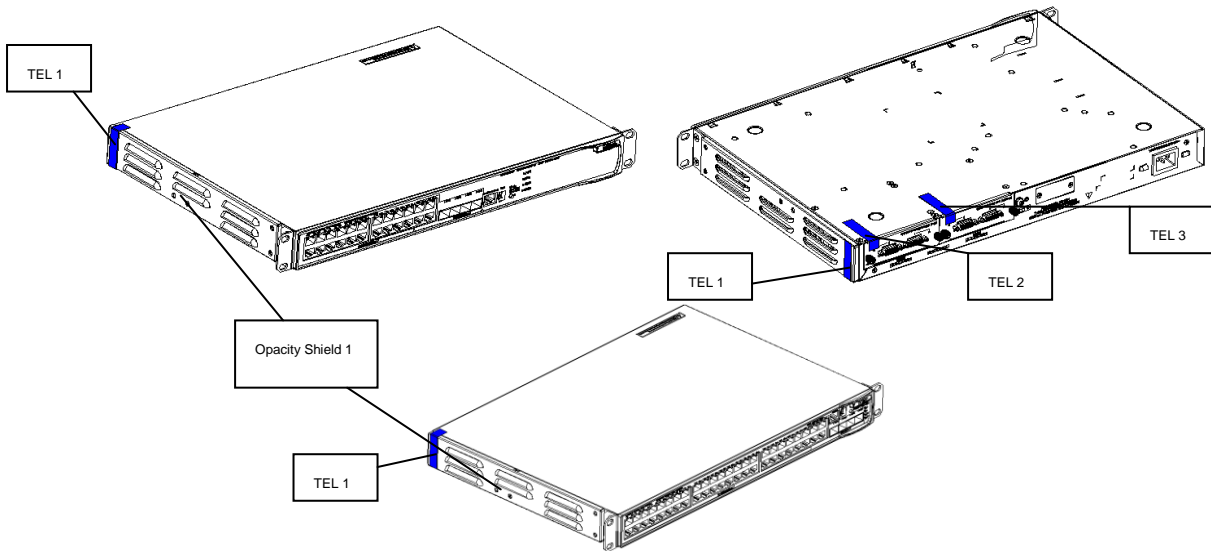


Figure 2 HP 5500 EI Switch Series Representative View

2.2.2 HP 5800 Switch Series

HP 5800 switches offer an unmatched combination of Gigabit and 10-Gigabit Ethernet port density, high-availability architecture, and full Layer 2 and Layer 3 dual-stack IPv4 and IPv6 capabilities. Besides wire-speed line-rate performance on all ports, the switches include patented IRF technology and Rapid Ring Protection Protocol (RRPP) that allow local or geographically distributed 5800 switches to be interconnected for higher resiliency and performance. Available in PoE and non-PoE models and 1U and 2U flex chassis configurations, 5800 switches are built on open standards and include an open application architecture (OAA) module slot that enables flexible deployment options for new services. These versatile switches are ideal for use in the network core for a building or department, or as a high-performance switch in the convergence layer or network edge of enterprise campus networks

Testing included six models in the 5800 series:

- HP 5800-24G
- HP 5800-24G-PoE+
- HP 5800-24G-SFP
- HP 5800-48G
- HP 5800-48G-PoE
- HP 5800-48G -2slot

Figure 3 shows representatives of the series. This series requires 6 Tamper-evident labels and 2 opacity shields for the 2 slot modules and 3 tamper-evident labels and 1 opacity shield for the 1 slot modules when configured as shown in Figure 3.

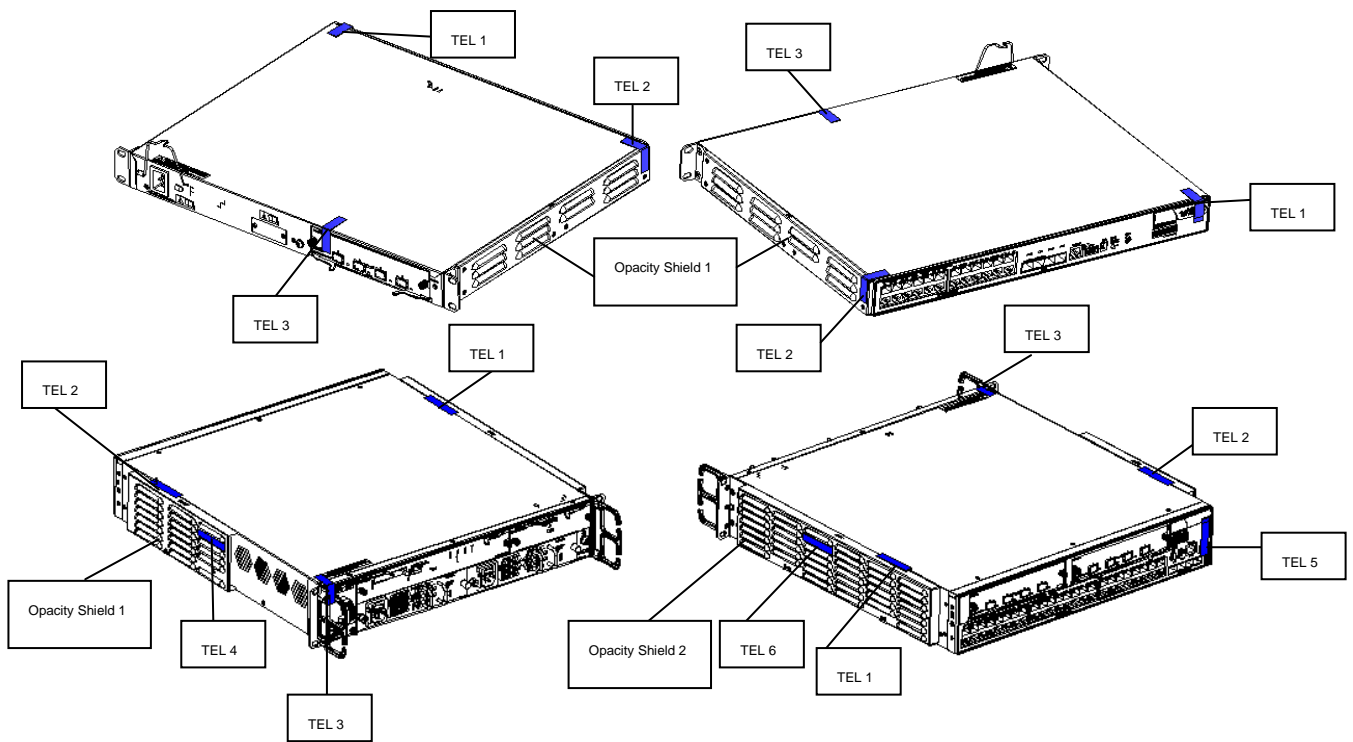


Figure 3 HP 5800 Switch Series Representative View

2.2.3 HP 5820 Switch Series

The HP 5820 Switch Series features advanced flex-chassis switches that deliver a unique combination of unmatched 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) connectivity, high-availability architecture, full Layer 2/3 dual-stack IPv4/v6, and line-rate, low-latency performance on all ports. Extensible embedded application capabilities enable these switches to integrate services into the network, consolidating devices and appliances to simplify deployment and reduce power consumption and rack space. Extremely versatile, the switches can be used in high-performance, high-density building or department cores as part of a consolidated network; for data center top-of-rack server access; or as high-performance Layer 3, 10-Gigabit Ethernet aggregation switches in campus and data center networks.

Testing included two models in the 5820 series:

- HP 5820-14XG-SFP
- HP 5820-24XG-SFP

Figure 4 shows representatives of the series. This series requires 6 Tamper-evident labels and 2 opacity shields for the 24XG modules and 5 tamper-evident labels and 2 opacity shield for the 14XG modules when configured as shown in Figure 4.

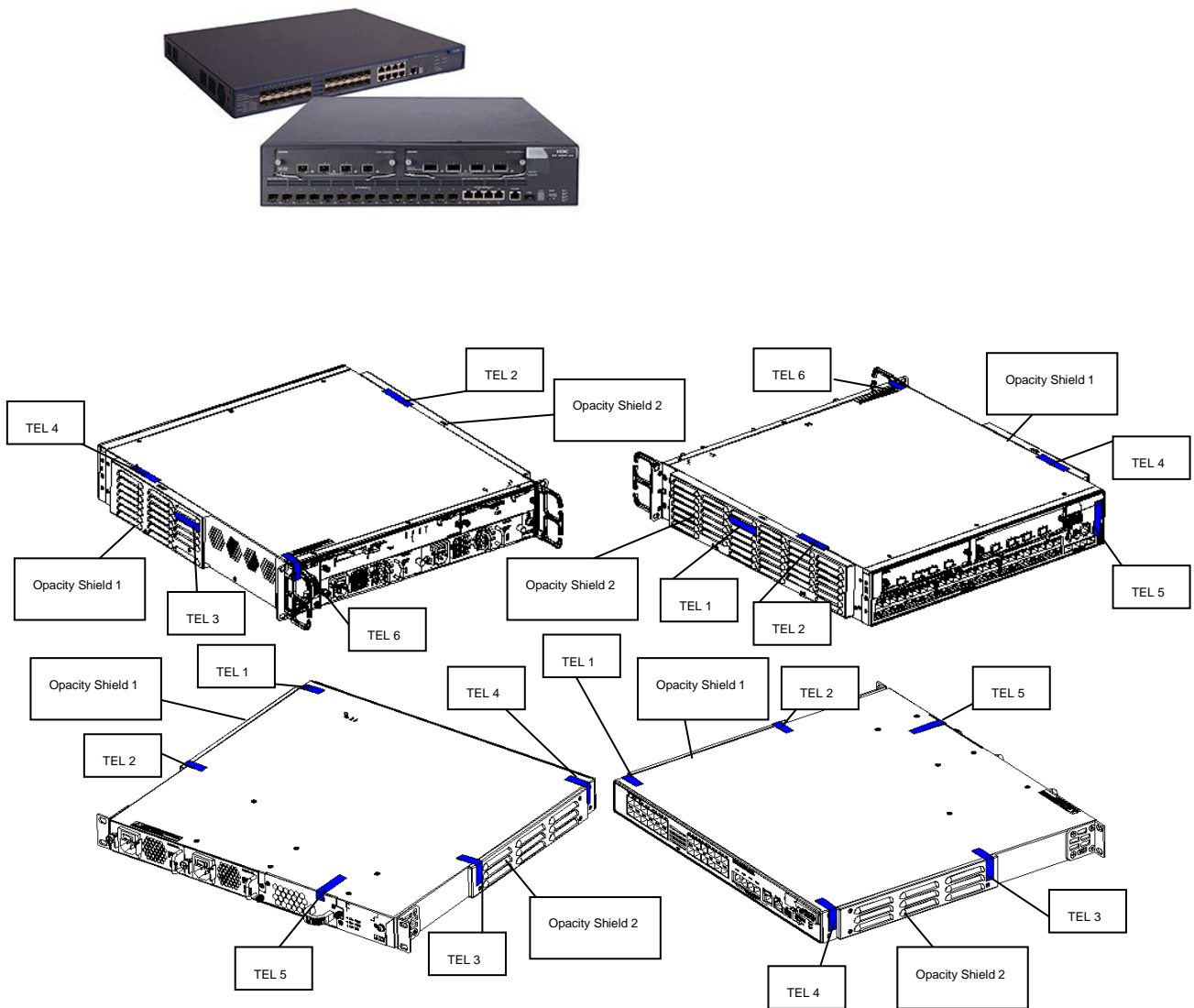


Figure 4 HP 5820 Switch Series Representative View

2.3 Modular Ethernet Switches

2.3.1 HP 7500 Switch Series

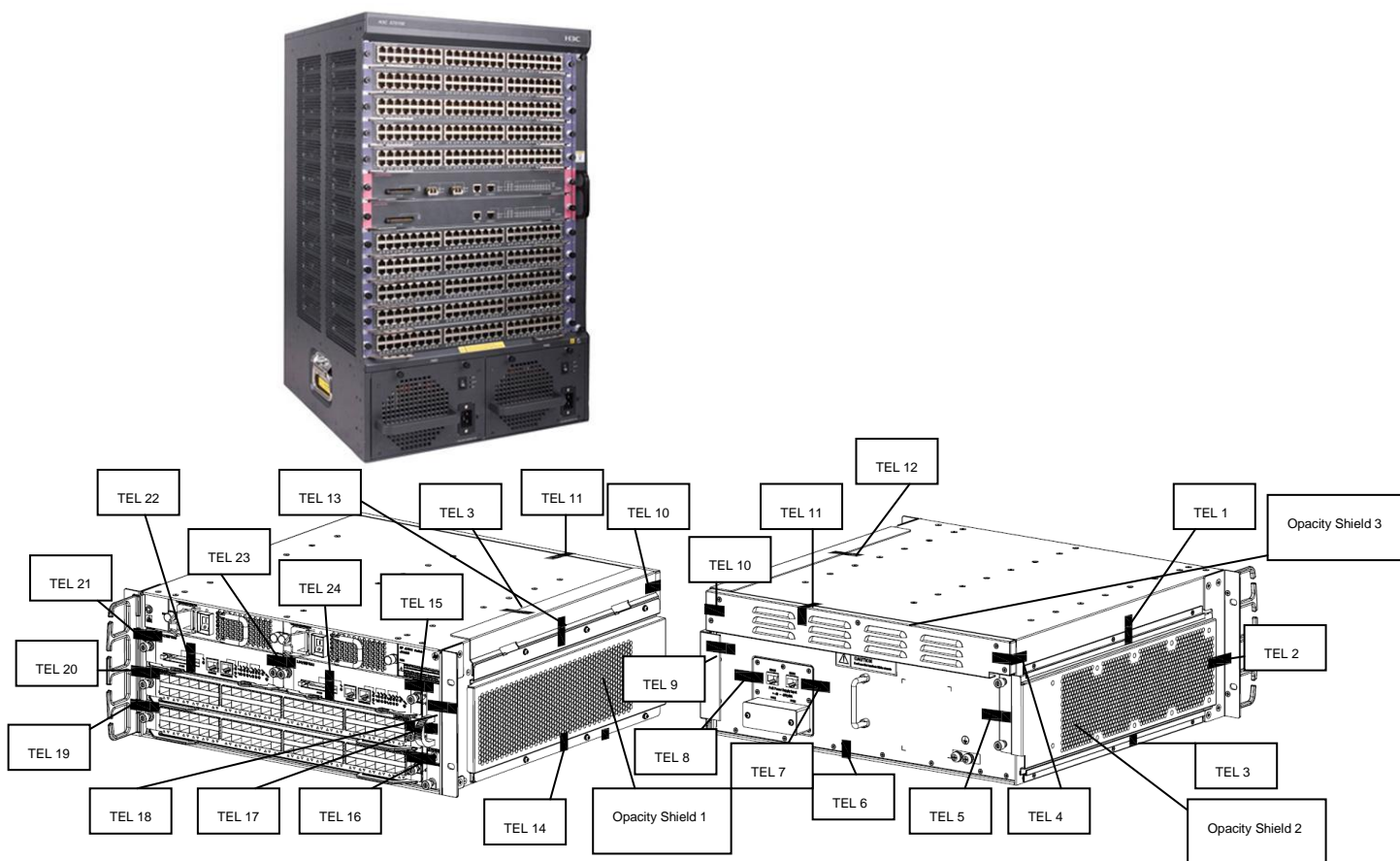
The HP 7500 Switch Series comprises 10-Gigabit modular core switches designed for the requirements of enterprise data center applications. These multilayer switches meet the evolving needs of integrated services networks, and can be deployed in multiple network environments, including the enterprise LAN core, aggregation layer, and wiring closet edge, as well as in metropolitan area networks (MANs) and data centers. They feature cost-effective wire-speed 10 Gigabit Ethernet ports to provide the throughput and bandwidth necessary for mission-critical data and high-speed communications. A passive backplane, support for load sharing, and redundant management and fabrics help HP 7500 series switches offer high

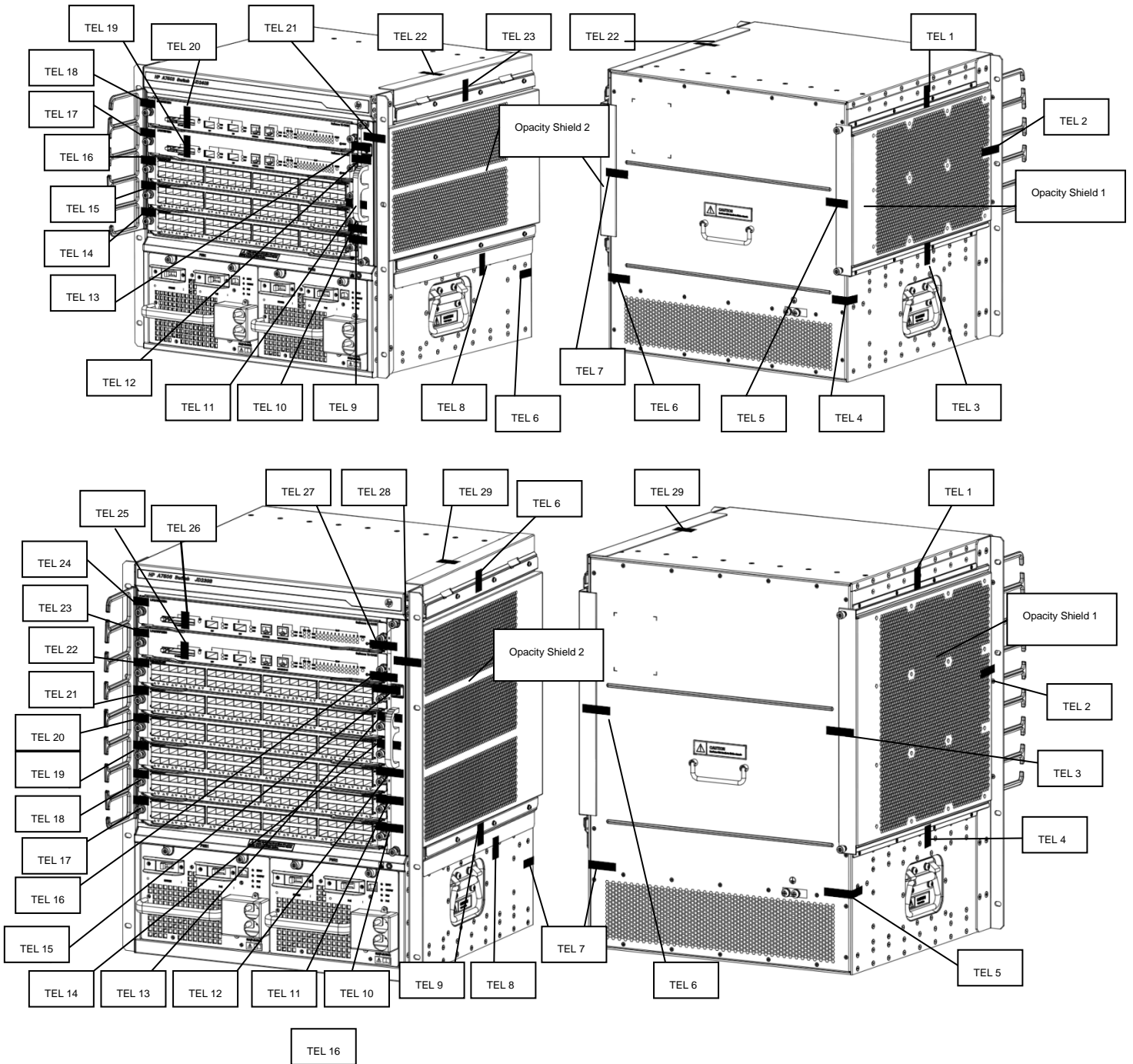
availability. Moreover, these switches deliver wire-speed Layer 2 and Layer 3 routing services for the most demanding applications.

Testing included six models in the 7500 series:

- HP 7510
- HP 7506
- HP 7506V
- HP 7503
- HP 7502
- HP 7503-S

Figure 5 shows a representative of the series. This series is illustrated below with 24 Tamper-evident labels and 3 opacity shields, 23 Tamper-evident labels and 2 opacity shields, 29 Tamper-evident labels and 2 opacity shields, 38 Tamper-evident labels and 5 opacity shields, and 39 Tamper-evident labels and 2 opacity shields, dependent on the number of card slots when configured as shown in Figure 5.





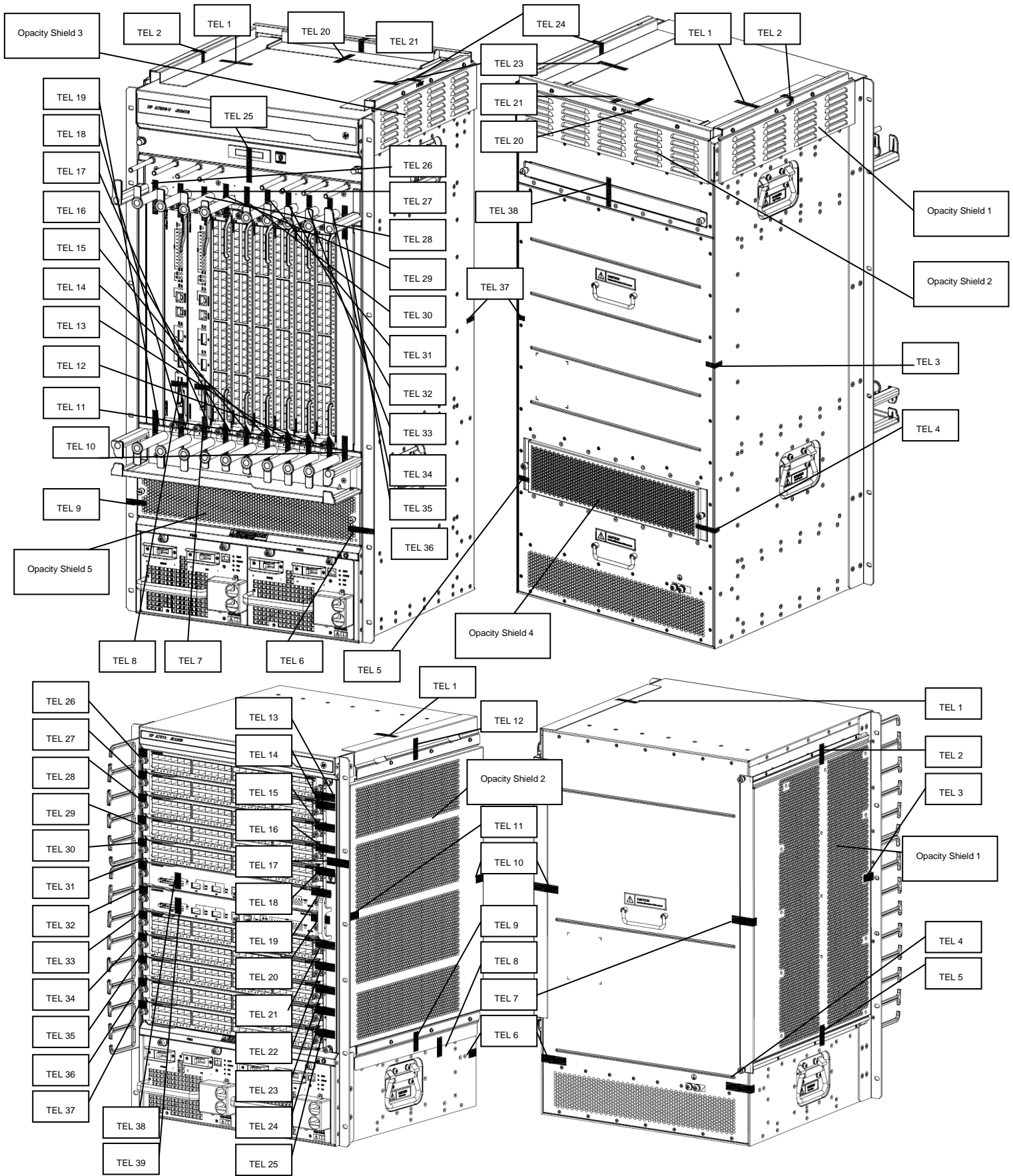


Figure 5 HP 7500 Switch Series Representative View

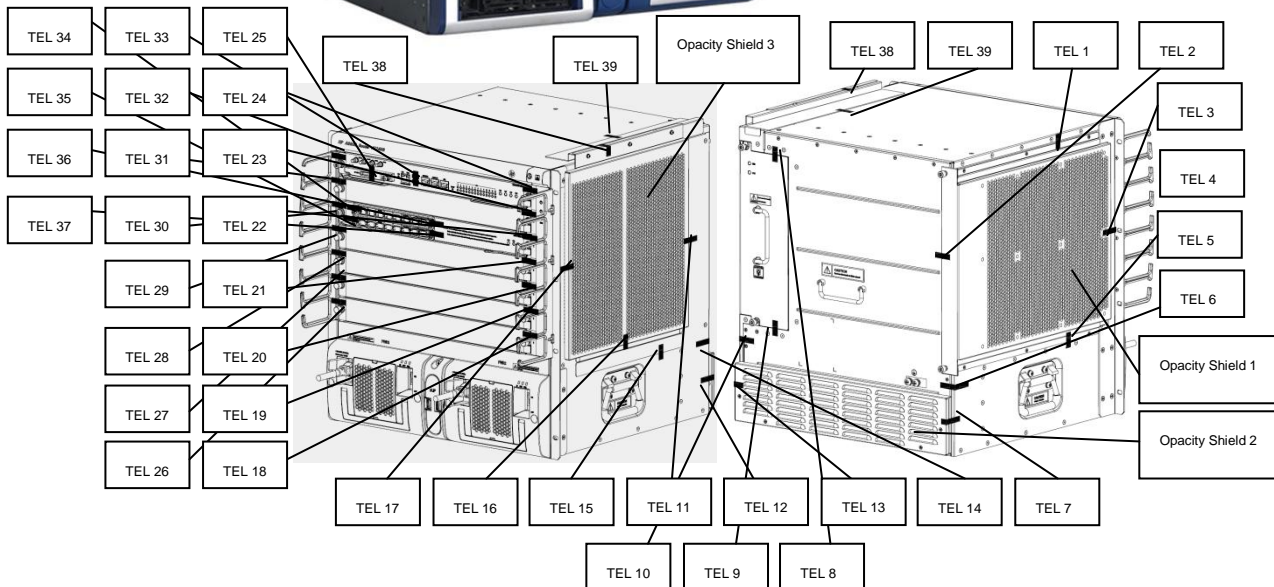
2.3.2 HP 9500 Switch Series

The HP 9500 Switch Series are modular switches that form a next-generation data center/large campus core switching platform. With unprecedented levels of networking performance, industry-leading availability, and flexible and efficient deployment options, these switches enable new services while driving down the cost of network operations. The 9500 series switches can provide more than 1.4 TB of high-performance switching capacity, aggregate up to 192 10-Gigabit Ethernet or 576 Gigabit Ethernet ports, and offer a future-proof architecture that enables customers to support emerging enterprise core or data center requirements.

Testing included three models in the series:

- HP 9505
- HP 9508V
- HP 9512

Figure 6 shows a representative of the series. This series requires 39 Tamper-evident labels and 3 opacity shields, 47 Tamper-evident labels and 3 opacity shields, and 54 Tamper-evident labels and 3 opacity shields for the modules when configured as shown in Figure 6.



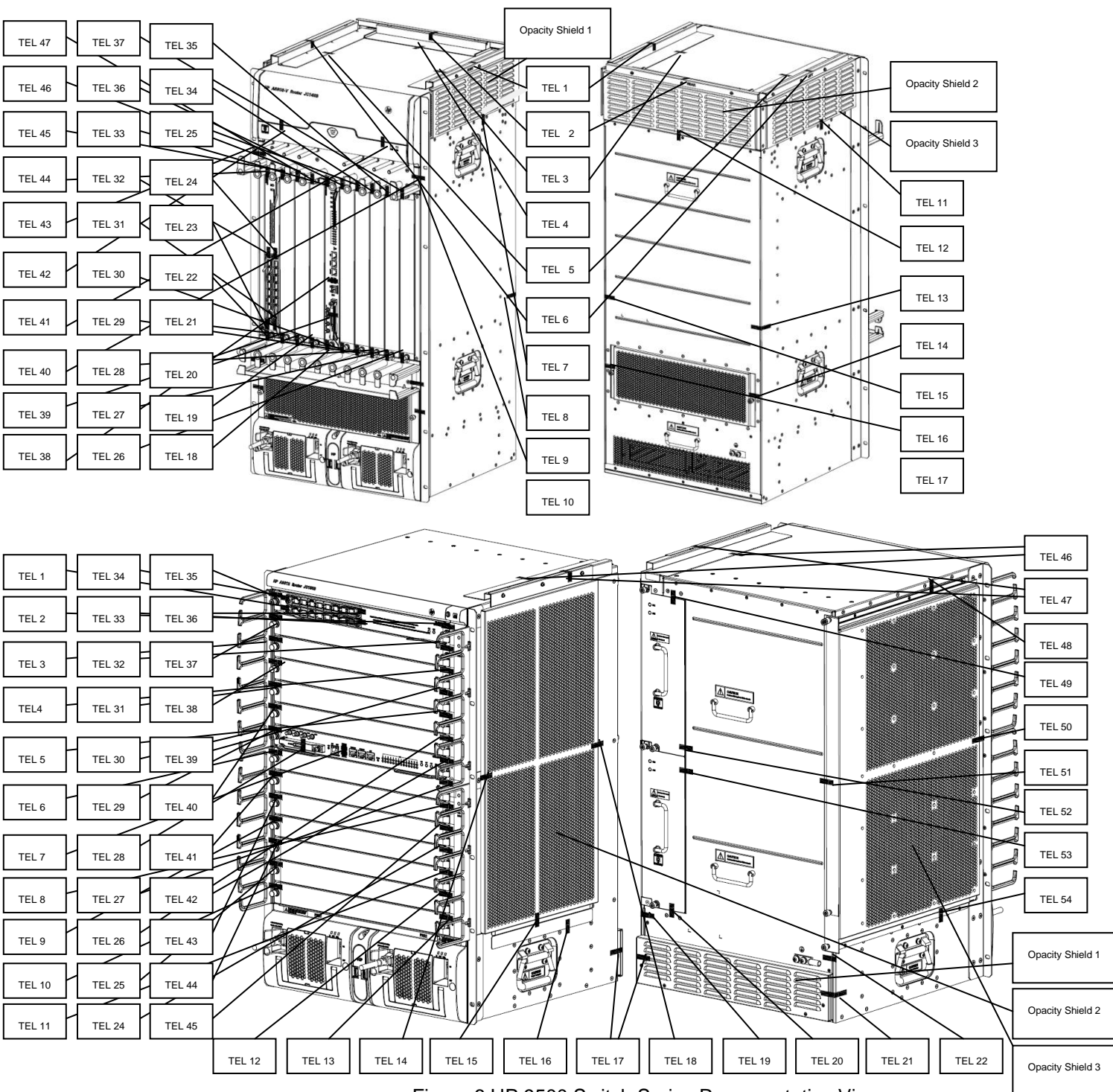


Figure 6 HP 9500 Switch Series Representative View

2.3.3 HP 12500 Switch Series

The HP 12500 Switch series comprises a pair of powerful, next-generation routing switches with outstanding capacity for the network core or the data center. Besides innovative IRF technology that provides unprecedented levels of performance and high availability, HP 12500 series switches incorporate the OAA, which enables flexible deployment options for new services. These switches also have energy-efficiency features that drive down operational expenses. The 12500 series is ideal for organizations contemplating large-scale data center or campus consolidations, business continuity and disaster recovery sites, metropolitan area network deployments, and other applications requiring a robust, high-performance switching platform.

- Advanced multi-level, multi-plane non-blocking switching architecture.

- Ultra-high port density and support for multiple interface types including the XFP 10-Gigabit Ethernet optical interface, SFP Gigabit Ethernet optical interface, and 10/100/1000 Mbps electrical interface.
- Future-proof design, allowing the series to provide in the future value-added security services like firewall, IPSec, and LB to meet the requirements of intelligent IP networks.

The 12500 series are mainly deployed at:

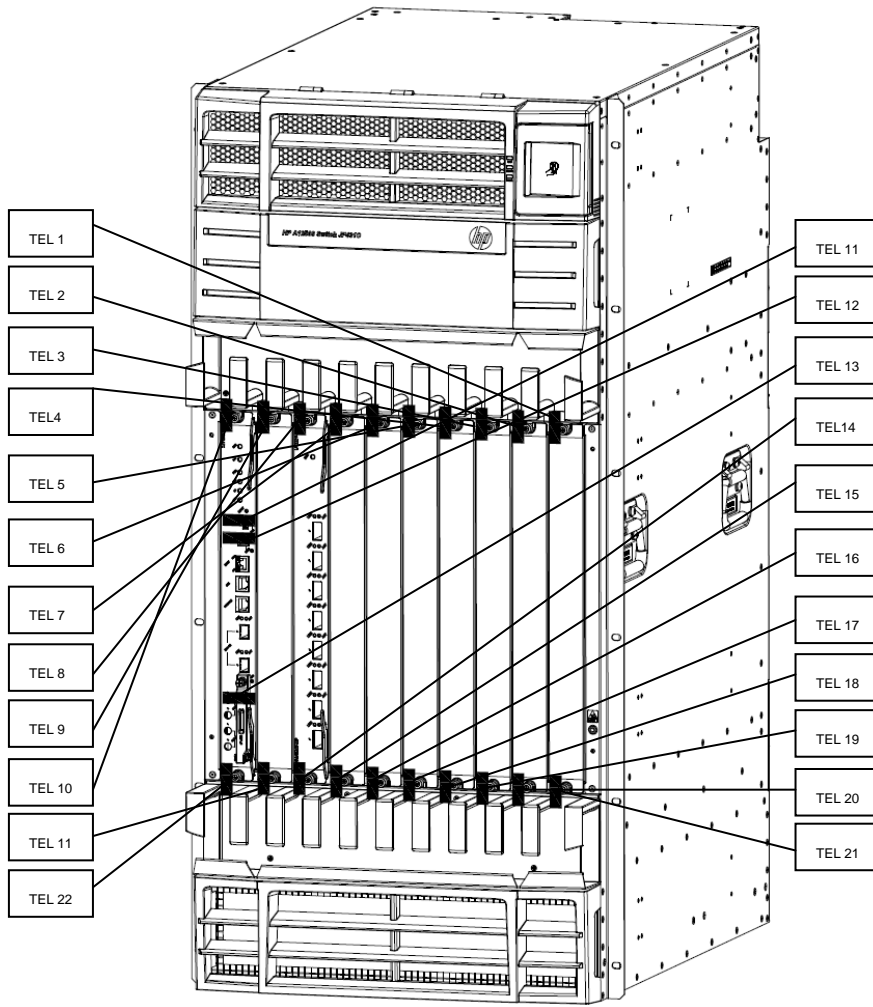
- Core layer and distribution layer of large-scale data centers (DCs)
- Core layer of large-scale industry networks and campus networks
- Large clusters and grid computing

Testing included two models in the 12500 series:

- HP 12508
- HP 12518

Figure 7 shows a representative of the series. This series requires 22 Tamper-evident labels and 43 Tamper-evident labels for the modules when configured as shown in Figure 7





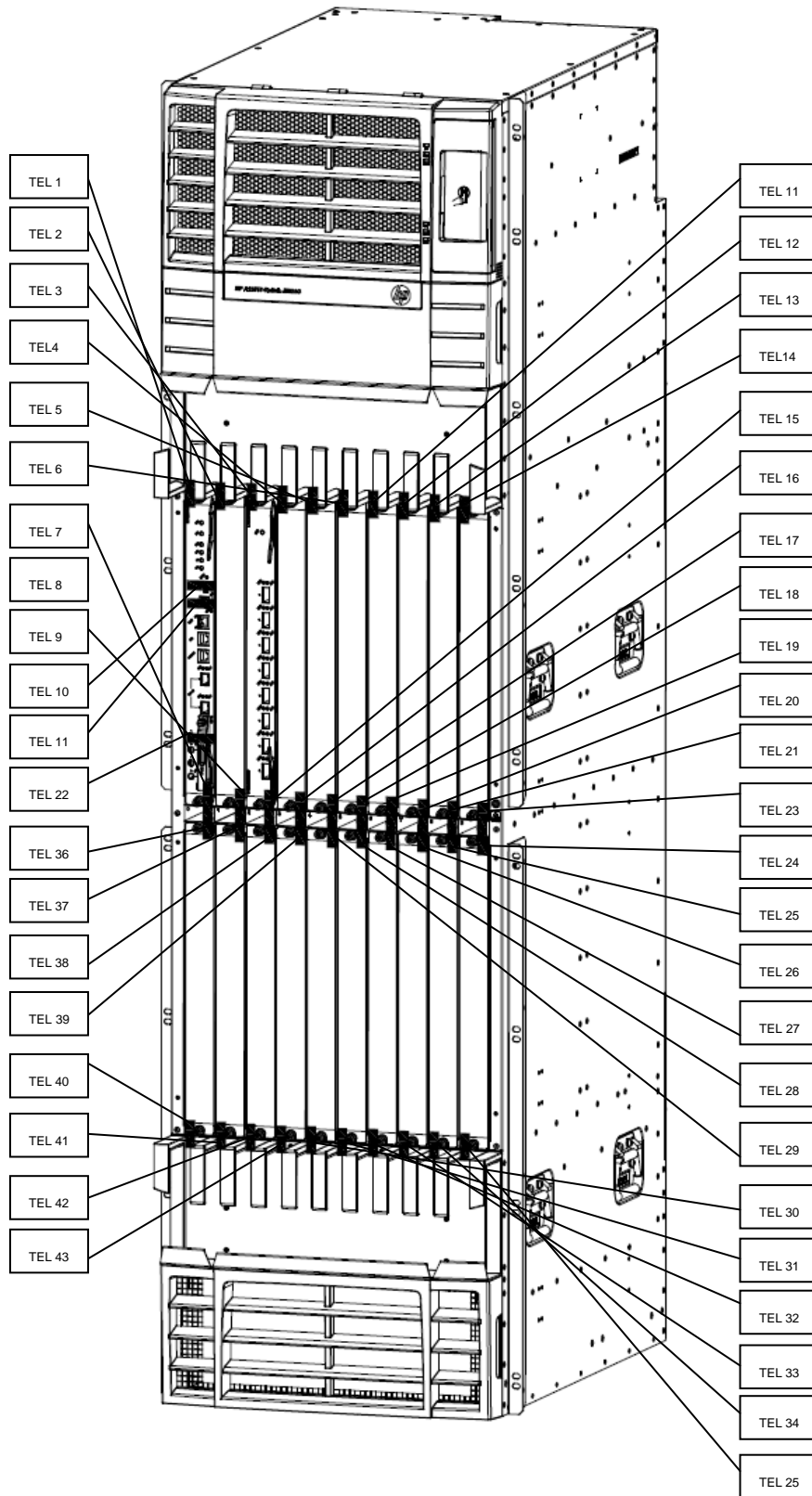


Figure 7 HP 12500 Switch Series Representative View

3 Security Appliance Validation Level

Table 1 lists the level of validation for each area in the FIPS PUB 140-2.

Table 1 Validation Level by Section

| No. | Area | Level |
|-----|---|-------|
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key management | 2 |
| 8 | Electromagnetic Interface/Electromagnetic Compatibility | 2 |
| 9 | Self-Tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

4 Physical Characteristics and Security Appliance Interfaces

4.1 Fixed-port L2/L2+ Managed Ethernet Switches

Each HP 5120-EI switch is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case. The general components of the HP 5120-EI switches include firmware and hardware, which are placed in the three-dimensional space within the case.

4.1.1 HP 5120-EI Switch Series

HP 5120-EI switches provide 24 or 48 Gigabit Ethernet ports including models with PoE. Each switch has four Gigabit SFP ports, which form combo ports with the last four Ethernet ports. The tested devices have two slots for pluggable modules. Modules provide one or two 10-Gigabit Ethernet interfaces (SFP+, XFP, and CX4 formats). Port status LEDs together with a port mode LED indicate the state of each port (rate, duplex, power, and failures).

In addition, each 5120-EI switch has a serial console port for management and LEDs for system, power, and module status. Each has an AC power input while PoE models have an additional redundant power supply (RPS) input.

http://h17007.www1.hp.com/us/en/products/switches/HP_5120_EI_Switch_Series/index.aspx#ab2 describes the ports in detail along with the interpretation of the LEDs.

4.2 Fixed-port L3 Managed Ethernet Switches

Each HP 5500-EI, 5800, and 5820 switch is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case. The general components of the HP 5500-EI, 5800, and 5820 switches include firmware and hardware, which are placed in the three-dimensional space within the case.

4.2.1 HP 5500-EI Switch Series

HP 5500-EI switches provide 24 Gigabit Ethernet, 48 Gigabit Ethernet or 24 SFP ports. The series includes models with PoE. Each Gigabit Ethernet switch has four Gigabit SFP ports, which form combo ports with the last four Ethernet ports. The SFP switch has eight Gigabit Ethernet ports, which form combo ports with the last eight SFP ports. The tested devices have two slots for pluggable modules. Modules provide one or two 10-Gigabit Ethernet interfaces (SFP+, XFP, and CX4 formats). Port status LEDs together with a port mode LED indicate the state of each port (rate, duplex, power, and failures).

In addition, each 5500-EI switch has a serial console port for management and LEDs for system, power, and module status. Each has an AC power input while PoE models have an additional RPS input. The SFP switch has two slots for hot-swappable power supplies (only one power supply is provided).

http://h17007.www1.hp.com/us/en/products/switches/HP_5500_EI_Switch_Series/index.aspx#ab2 describes the ports in detail along with the interpretation of the LEDs.

4.2.2 HP 5800 Switch Series

HP 5800 switches provide both SFP and Gigabit Ethernet ports, along with slots for pluggable modules. The 5800-24G SFP model has 24 SFP Gigabit ports, four SFP+ 10-Gigabit ports, and one slot for pluggable modules. The other 5800 models have either 24 or 48 Gigabit Ethernet ports with either four SFP+ 10-Gigabit or four SFP Gigabit ports. Gigabit Ethernet modules support PoE. All models have one slot for a pluggable module, with an additional slot available on a 48-port model (which also has a slot for an Open Application Platform (OAP) card). Pluggable modules provide options for additional ports including 16 Gigabit Ethernet ports, 16 SFP Gigabit ports, or up to four SFP+ 10-Gigabit ports. Port status LEDs together with a port mode LED indicate the state of each port (rate, duplex, power, and failures).

In addition, each 5800 switch has a serial console port for management. Model 5800-24G SFP has an additional management Gigabit Ethernet port. The switches have LEDs for system, power, and module status. 5800 switches have a USB 2.0 port. Each has an AC power input while PoE models have an additional RPS input. Some models support hot-swappable power modules.

http://h17007.www1.hp.com/us/en/products/switches/HP_5800_Switch_Series/index.aspx#tab2 describes the ports in detail along with the interpretation of the LEDs.

4.2.3 HP 5820 Switch Series

HP 5820 switches provide either 14 or 24 SFP+ 10-Gigabit ports with four Gigabit Ethernet ports. Model 5820-14XG-SFP+ has two slots for pluggable modules and one slot for an OAP module. Modules have two or four SFP+ 10-Gigabit ports.

In addition, each 5820 switch has a serial console port for management and a USB port. Model 5820X-24XG has an additional management Ethernet port. The switches have LEDs for system, power, and module status. Each has an AC power input, with support for two power modules.

http://h17007.www1.hp.com/us/en/products/switches/HP_5820_Switch_Series/index.aspx#tab2 describes the ports in detail along with the interpretation of the LEDs.

4.3 Modular Ethernet switches

Each modular Ethernet switch is a multi-chip standalone security appliance. The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the integrated chassis. The general components of each modular Ethernet switch include firmware and hardware which are placed in the three-dimensional space within the chassis.

The modular Ethernet switches use a distributed architecture, which comprises the chassis, power module, fan, backplane, main processing units (MPUs), and line processing units (LPUs). A MPU is the core of a switch. It implements the following features:

- Calculate routes and maintain forwarding tables,
- Provide data exchange between LPUs (7500 and 9500),
- Provide system configuration and functions to monitor other boards as well as upgrade and reset board software,
- Support active/standby switchover.

4.3.1 HP 7500 Switch Series

HP 7500 chassis accommodate two, three, six or ten LPUs. LPUs provide Gigabit Ethernet, SFP Gigabit, and XFP 10-Gigabit ports in a range of numbers and combinations. The series supports a maximum of 480 Gigabit Ethernet ports or 480 SFP Gigabit ports, and 84 XFP 10-Gigabit ports. Each LPU has LEDs to indicate port status.

In addition, each 7500 switch requires a MPU¹. The chassis have two MPU slots (except for model 7503-S, which has one). Each MPU provides a serial console port and a 100 Mbps Ethernet port for management. MPUs provide additional combinations of ports including Gigabit Ethernet, SFP Gigabit, and XFP 10-Gigabit ports as well a compact flash (CF) card slot (Type I or II). The MPUs have status LEDs for LPUs, management port, network ports, CF, power, and fan tray status reporting. Each MPU has a reset button.

Each chassis has two slots for power modules. Each power module has a power input (AC or DC), a system power switch, and power LED. Some power modules provide PoE along with a PoE power switch, PoE status LEDs, and a console port to monitor PoE. The 7502 and 7503-S chassis provide inputs for external PoE power supplies together with monitoring ports (RS-485 and RS-232).

http://h17007.www1.hp.com/us/en/products/switches/HP_7500_Switch_Series/index.aspx describes MPU options, LPU options, and ports in detail along with the interpretation of the LEDs.

¹ MPU are also known as switching and routing processing unit (SRPU) for 7500 switches.

4.3.2 HP 9500 Switch Series

HP 9500 chassis accommodate five, eight or twelve LPUs. LPUs provide Gigabit Ethernet, SFP Gigabit, SFP+ 10-Gigabit, and XFP 10-Gigabit ports in a range of numbers and combinations. The series supports a maximum of 576 Gigabit Ethernet ports or 576 SFP Gigabit ports, and 192 SFP+ 10-Gigabit ports. Each LPU has LEDs to indicate port status.

In addition, each 9500 switch requires a MPU. The chassis have two MPU slots. Each MPU provides a 100 Mbps Ethernet management port, a serial management port, an auxiliary serial port, two USB ports (host and device), and a CF card slot. (The MPU have reserved ports, which are not supported at present (a RS-232/485 port and standby main board coaxial clock interfaces).) The MPU have status LEDs for MPU, LPUs, management port, USB ports, and CF status reporting. Each MPU has a reset button.

Each chassis has two slots for AC or DC power supply units (PSU). An AC PSU has slots for two sub-PSUs along with a switch for each sub-PSU. An AC sub-PSU has AC input and power LEDs. A DC PSU has power input, power switch, and status LEDs.

http://h17007.www1.hp.com/us/en/products/switches/HP_9500_Switch_Series/index.aspx#tab2 describes MPU options, LPU options, and ports in detail along with the interpretation of the LEDs.

4.3.3 HP 12500 Switch Series

HP 12500 chassis accommodate eight or eighteen LPUs. LPUs provide Gigabit Ethernet, SFP Gigabit, SFP+ 10-Gigabit, and XFP 10-Gigabit ports in a range of numbers and combinations. The series supports a maximum of 864 Gigabit Ethernet ports or 864 SFP Gigabit ports, and 512 SFP+ 10-Gigabit ports. Each LPU has LEDs to indicate port status.

In addition, each 12500 switch requires a MPU. The chassis have two MPU slots. Each MPU provides a 100-Mbps Ethernet management port, a serial management port, an auxiliary serial port, two USB ports (host and device), and a CF card slot. (The MPUs have reserved ports, which are not supported at present (a RS-232/485 port, standby main board coaxial clock interfaces, and MCC Gigabit Ethernet interfaces).) The MPUs have status LEDs for switching fabric modules, LPU, fan, power, MPU, and CF status reporting. Each MPU has a reset button.

Chassis power is provided through AC power frames (one for model 12508 and two for model 12518). Each AC power frame accommodates up to six hot-swappable 1U AC PSU. The frame as status LED and a power frame switch. A power entry module supplies power input to each PSU.

http://h17007.www1.hp.com/us/en/products/switches/HP_12500_Switch_Series/index.aspx#tab2 describes MPU options, LPU options, and ports in detail along with the interpretation of the LEDs.

4.4 Physical Interfaces Mapping

The physical interfaces provided by the HP Networking switches map to four FIPS 140-2 defined logical interface: data input, data output, control input and status output. Table 1 presents the mapping.

Table 1 Correspondence between Physical and Logical Interfaces

| Physical Interface | FIPS 140-2 Logical Interface |
|--------------------|------------------------------|
| Networking ports | Data Input Interface |
| Console port | |

| Physical Interface | FIPS 140-2 Logical Interface |
|---------------------------------------|------------------------------|
| Management Ethernet port | |
| CF card slot | |
| Networking ports | Data Output Interface |
| Console port | |
| Management Ethernet port | |
| CF card slot | |
| Networking ports | Control Input Interface |
| Console port | |
| Management Ethernet port | |
| Power switches | |
| Reset Switch | |
| Port status LED mode switching button | |
| Networking ports | Status Output Interface |
| Console port | |
| Management Ethernet port | |
| LEDs | |
| Power Slot | Power Interface |
| Backplane | |
| USB ports | Unused Interface |
| AUX port | |
| SMB coaxial clock interfaces | |
| RS-232/485 interfaces | |

5 Roles, Services, and Authentication

5.1 Roles

The HP Networking switches provide four roles: Visit, Monitor, Config, and Manage. Roles Visit, Monitor, and Config correspond to the FIPS 140-2 User Role. The Manage role corresponds to the FIPS 140-2 Crypto Officer role. The devices allow multiple management users to operate the appliance simultaneously.

The HP Networking switches do not employ a maintenance interface and do not have a maintenance role.

5.2 Services

HP Networking switches provide six classes of services:

- View device status,
- Network functions,
- Security management,
- Review the audit trail,
- View running status, and
- Configure the security appliance.

You can access these services by using any of the following methods:

- Console Port
- SSH
- Web user interface via HTTPS

The console port and SSH present a command line interface while the web user interface is a graphical user interface. The following table lists services available to each role within each class of service. The role in the brackets is the corresponding role specified in FIPS 140-2. HP Networking switches do not support bypass (that is, services provided without cryptographic processing).

Table 2 Services by Role

| Role | Privilege level | Services |
|---------------------|-----------------|---|
| Visit [User role] | 0 | 1) View device status: Currently running image version; Installed hardware components status and version. 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level. |
| Monitor [User role] | 1 | 1) View device status: Currently running image version; Installed hardware components status and version 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level. 4) Review the audit trail; |
| Config [User role] | 2 | 1) View device status: Currently running image version; Installed hardware components status and version 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level; Reset and change the password of same/lower privilege user; Maintenance of the super password; Maintenance (create, destroy, import, export) of public key/private key/shared key. 4) Review the audit trail 5) View running status: Memory status, Packet statistics, |

| Role | Privilege level | Services |
|------------------------------|-----------------|--|
| | | <p>Interface status, Current running Image version, Current configuration, Routing table, Active sessions, Temperature, SNMP MIB statistics.</p> <p>6) Configure the security appliance: Save configuration; Management of information center (start-up and shut down audit functions; setting logbuffer, setting logfile; setting log output destination); Managing (create, modify, delete apply) the filtering rules; Management of firewall; Define network interfaces and settings; Set the protocols the security appliance will support; enable interfaces and network services.</p> |
| Manage [Crypto Officer role] | 3 | <p>1) View device status: Currently running image version; Installed hardware components status and version</p> <p>2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client.</p> <p>3) Security management: Change the privilege level; Reset and change the password of same/lower privilege user; Maintenance of the super password; Maintenance (create, destroy, import, export) of public key/private key/shared key; Shut down or Reboot the security appliance; Management (create, delete, modify) of the user group; Management (create, delete, modify) of the user account; Management of the time; Maintenance (delete, modify) system start-up parameters;</p> |

| Role | Privilege level | Services |
|------|-----------------|---|
| | | <p>File operation (e.g. dir, copy, del); Management of the command privilege; Install or remove HP Networking Security Appliance.</p> <p>4) Review the audit trail;</p> <p>5) View running status: Memory status, Packet statistics, Interface status, Current running image version, Current configuration, Routing table, Active sessions, Temperature, SNMP MIB statistics.</p> <p>6) Configure the security appliance: Save configuration; Management of information center (start-up and shut down audit functions; setting logbuffer, setting logfile; setting log output destination delete of the audit trail.); Managing (create, modify, delete apply) the filtering rules; Management of firewall; Define network interfaces and settings; Set the protocols the security appliance will support (e.g. SFTP server, SSH server); enable interfaces and network services; Management of access control scheme (e.g. domain and RADIUS scheme).</p> |

http://h17007.www1.hp.com/us/en/products/switches/HP_12500_Switch_Series/index.aspx#tab_2 provides details of the commands that provide the services listed in Table 2. http://h17007.www1.hp.com/us/en/products/switches/HP_12500_Switch_Series/index.aspx#tab_2) presents the corresponding web user interface.

5.3 Authentication Mechanisms

HP Networking switches support both role-based and identity-based authentication.

- Identity-based authentication

Each user is authenticated upon initial access to the device. The authentication is

identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

To logon to the appliances, an operator must connect to it through one of the management interfaces (console port, SSH, HTTPS) and provide a password.

- Role-based authentication

Each User can switch to a different user privilege level without logging out and terminating the current connection. To switch to a different privilege level, a user must provide the privilege level switching authentication information. The authentication is role-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

After the privilege level switching, users can continue to manage the device without relogging in, but the commands they can execute have changed. For example, with the user privilege level 3, a user can configure system parameters as crypto officer role. After switching to user privilege level 0, the user can execute only basic commands like ping and tracert and use a few display commands as user role.

Operators must be authenticated using user names and passwords. The passwords must:

- 1) Be a minimum of six characters long, and the maximum password size is 63.
- 2) Be a combination of alphabetic and numeric characters.
- 3) Contain punctuation characters.
- 4) Contain lower and upper case characters.

The probability of a false positive for a random password guess is less than 1 in 1,000,000. This is also valid for RADIUS or TACACS+ shared secret keys

The users who try to log in or switch to a different user privilege level can be authenticated by RADIUS and TACACS+ Server. The device (RADIUS client) and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords exchanged between them. For more details, see RFC 2865: 3 Packet Format Authenticator field and 5.2 User-password

6 Approved Cryptographic Algorithms

Table 3 lists the FIPS-Approved algorithms HP Networking switches provide.

Table 3 FIPS-Approved Cryptography Algorithms

| Algorithm | Application | Certificate |
|---------------|--|-------------|
| AES | Encryption/decryption | 1927 |
| Triple-DES | Encryption/decryption | 1254 |
| SHA-1 | SHA-1 hashing | 1692 |
| SHA-256 | SHA-256 hashing | |
| HMAC SHA1 | SHA-1 HMAC for hashed message authentication | 1161 |
| HMAC SHA256 | SHA-256 HMAC for hashed message authentication | |
| RSA | Signing and verifying | 993 |
| DSA | Signing and verifying | 611 |
| X9.31 for RNG | Random number generation | 1014 |
| TLS | For Layer 7 security | |

7 Non-approved Cryptographic Algorithms

HP Networking switches provide additional cryptographic algorithms that are not FIPS Approved:

- DES
- RC4
- MD5
- MD5 HMAC
- RSA (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)

8 Cryptographic Key Management

The security appliances use a variety of Critical Security Parameters (CSP) during operation. Table 4 lists the CSP including cryptographic keys used by the HP Networking security switches. It summarizes generation, storage, and zeroization methods for the CSP.

Table 4 Cryptographic Security Parameters

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|---|------------------|--------------------------|-------------|---------|-------------|
|---|------------------|--------------------------|-------------|---------|-------------|

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|------|-----------------------------|---|---|--|---|
| CSP1 | RSA public/ private keys | ANSI X9.31/RSA | Identity certificates for the security appliance itself and also used in TLS and SSH negotiations. The security appliance supports 1024 ~ 2048 bit key sizes. | Private Key-FLASH (cipher text/Triple-DES) and RAM (plain text) Public Key-FLASH (cipher text/ Triple-DES) and RAM (plain text) | Private Key - Using CLI command to zeroize, then reboot. Public Key - Using CLI command to zeroize, then reboot. |
| CSP2 | DSA public/ private keys | ANSI X9.31/DSA | Identity certificates for the security appliance itself and also used in SSH negotiations. | Private Key-FLASH (cipher text/Triple-DES) and RAM (plain text) Public Key-FLASH (cipher text/Triple-DES) and RAM (plain text) | Private Key-Using CLI command to zeroize, then reboot. Public Key - Using CLI command to zeroize, then reboot. |
| CSP3 | Diffie-Hellman Key Pairs | ANSI X9.31 / DH | Key agreement for TLS, and SSH sessions. | RAM (plain text) | Resetting or rebooting the security appliance. |
| CSP4 | Public keys | DSA / RSA | Public keys of peers | FLASH(plain text)/ RAM (plain text) | Delete public keys of peers from configuration, write to startup config, then reboot |
| CSP5 | TLS Traffic Keys | Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + either DH or RSA) Algorithm: Also Triple-DES & AES | Used in HTTPS connections | RAM (plain text) | Resetting or rebooting the security appliance. |
| CSP6 | SSH Session Keys | ANSI X9.31 / Triple-DES-AES | SSH keys | RAM (plain text) | Resetting or rebooting the security appliance |
| CSP7 | IPSec authentication keys | Triple-DES-AES | Triple-DES or AES Keys are manually configured for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP. | FLASH(plain text) / RAM (plain text) | Delete IPSec keys from configuration, write to startup config, then reboot |
| CSP8 | IPSec traffic keys | Triple-DES-AES | Triple-DES or AES Keys are manually configured for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP. | FLASH(plain text)/ RAM (plain text) | Delete IPSec keys from configuration, write to startup config, then reboot |

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|-------|---|--------------------------|---|---|--|
| CSP9 | RADIUS shared secret keys | Shared Secret | Used for authenticating the RADIUS server to the security appliance and vice versa. Entered by the Crypto-Officer in plain text form and stored in plain text form. | FLASH (plain text) and RAM (plain text) | Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot. |
| CSP10 | Username/ Passwords/ super password | Secret | Critical security parameters used to authenticate the administrator login or privilege promoting. | FLASH (plain text) and RAM (plain text) | Overwriting the passwords with new ones, write to startup config, then reboot. |
| CSP11 | Certificates of Certificate Authorities (CAs) | ANSI X9.31 | Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates. | FLASH (plain text) and RAM (plain text) | 1. Delete PKI domain from configuration via erase flash: command, write to startup config, then reboot. 2. Use "pki delete-certificate" CLI command to delete certificates, then reboot |
| CSP12 | PRNG Seed Key | Entropy | Seed key for X9.31 PRNG | RAM (plain text) | Zeroized with generation of new seed |

8.1 Access Control Policy

Table 5, Table 6, and Table 7 list by role services accessing CSPs. Each table identifies the services that access each CSP along with the type of access allowed for the role(s). The types of access are: read (r), write (w), and delete (d).

Table 5 CSP Access by Service for Visit and Monitor Roles

| Service Access /CSP | View device status | Network functions | Security management |
|---------------------|--------------------|-------------------|---------------------|
| CSP1 | r | r | R |
| CSP2 | r | r | R |
| CSP3 | r | r | R |
| CSP4 | r | r | R |
| CSP5 | r | r | R |
| CSP6 | r | r | R |
| CSP7 | r | r | R |
| CSP8 | r | r | R |
| CSP9 | r | r | R |

| Service Access /CSP | View device status | Network functions | Security management |
|---------------------|--------------------|-------------------|---------------------|
| CSP10 | r | r | R |
| CSP11 | r | r | R |
| CSP12 | r | r | R |

r = read, w = write, d = delete

Table 6 Access by Service for Config Role

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP1 | r | r | Rwd | r | r | r |
| CSP2 | r | r | Rwd | r | r | r |
| CSP3 | r | r | Rwd | r | r | r |
| CSP4 | r | r | Rwd | r | r | r |
| CSP5 | r | r | Rwd | r | r | r |
| CSP6 | r | r | Rwd | r | r | r |
| CSP7 | r | r | Rwd | r | r | r |
| CSP8 | r | r | Rwd | r | r | r |
| CSP9 | r | r | R | r | r | r |
| CSP10 | r | r | Rwd | r | r | r |
| CSP11 | r | r | Rwd | r | r | r |
| CSP12 | r | r | Rwd | r | r | r |

Table 7 Access by Service for Manage Role

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP1 | r | r | Rwd | r | r | r |
| CSP2 | r | r | Rwd | r | r | r |
| CSP3 | r | r | Rwd | r | r | r |

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP4 | r | r | Rwd | r | r | r |
| CSP5 | r | r | Rwd | r | r | r |
| CSP6 | r | r | Rwd | r | r | r |
| CSP7 | r | r | Rwd | r | r | r |
| CSP8 | r | r | Rwd | r | r | r |
| CSP9 | r | r | Rwd | r | r | r |
| CSP10 | r | R | Rwd | r | r | r |
| CSP11 | r | R | Rwd | r | r | r |
| CSP12 | r | R | Rwd | r | r | r |

9 Self-Tests

HP Networking switches include an array of self-tests that are run during startup and during operations to prevent any secure data from being released and to insure all components are functioning correctly.

9.1 Power-On Self-Tests

Table 8 lists the power-on self-tests implemented by the switches. The switches perform all power-on self-tests automatically at boot when FIPS mode is enabled. All power-on self-tests must be passed before any role can perform services. The power-on self-tests are performed prior to the initialization of the forwarding function, which prevents the security appliance from passing any data during a power-on self-test failure.

Table 8 HP Networking Switch Power-On Self-Tests

| Implementation | Tests Performed |
|-----------------------------|----------------------------------|
| Security Appliance Software | Software/firmware Test |
| | DSA KAT (signature/verification) |
| | RSA KAT (signature/verification) |
| | RSA KAT (encrypt/decrypt) |
| | AES KAT |
| | Triple-DES KAT |
| | SHA-1 KAT |
| | HMAC SHA-1 KAT |
| PRNG KAT | |

9.2 Conditional Self-Tests

Table 9 lists the conditional self-tests implemented by the switches. Conditional self tests run when a switch generates a DSA or RSA key pair and when it generates a random number.

Table 9 HP Networking Switch Conditional Self-Tests

| Implementation | Tests Performed |
|-----------------------------|---|
| Security Appliance Software | Pairwise consistency test for RSA |
| | Pairwise consistency test for DSA |
| | Continuous Random Number Generator Test for the FIPS-approved RNG (X9.31) |

10 Delivery and Operation

10.1 Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the Networking switch physical package and check as follows:

- Outer Package Inspection

- 1) Check that the outer carton is in good condition.
- 2) Check the package for a HP Quality Seal or IPQC Seal, and ensure that it is intact.
- 3) Check that the IPQC seal on the plastic bag inside the carton is intact.
- 4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.

- Packing List Verification

Check against the packing list for discrepancy in material type and quantity. If any discrepancy found, the goods shall be treated as DOA goods.

- External Visual Inspection

Inspect the cabinet or chassis for any defects, loose connections, damages, and illegible marks. If any surface defect or material shortage found, the goods shall be treated as DOA goods.

- Confirm Software/firmware

- 1) Version verification

To verify the software version, start the appliance, view the self test result during startup, and use the display version command to check that the software version is Comware software, Version 5.2, Release 1002(CC). 'FIPS1402&CC' indicate it is a FIPS 140-2 and CC certification version. If software loading failed or the version information is incorrect, please contact HP for support.

- 2) SHA-256 verification

To verify that software/firmware has not been tampered, run SHA Hash command on the appliance. If the hash value is different from release notes of this software, contact HP for support. To get release notes, please access HP website:

- DOA (Dead on Arrival)

If the package is damaged, any label/seal is incorrect or tampered, stop unpacking the goods, retain the package, and report to HP for further investigation. The damaged goods will be replaced if necessary.

10.2 Secure Operation

The rules for securely operating an HP Networking switch in FIPS mode are:

- 1) Install and connect the device according to the installation and configuration guides.
- 2) Start the device, and enter the configuration interface.
- 3) Check and configure the clock.
- 4) By default, the device does not run in FIPS mode. Enable the device to work in FIPS mode using the **fips mode enable** command in system view. This will allow the switch to internally enforce FIPS-compliance behavior, such as run power-up self-test and conditional self-test.
- 5) Delete all MD5-based digital certificates.
- 6) Delete the DSA key pairs that have a modulus length of less than 1024 bits and all RSA key pairs.
- 7) Set up username/password for crypto officer role and user role. Each password must comprise no less than 6 characters and must contain uppercase and lowercase letters, digits, and special characters.
- 8) Save the configurations and re-start the device.
The device works in FIPS mode after restarting:
- 9) Configure the security appliance to use SSHv2.
- 10) Configure the security appliance to use HTTPS for performing system management.

An operator can determine whether a switch is in FIPS mode with the command **display fips status**. When in FIPS mode:

- The FTP/TFTP server is disabled.
- The Telnet server is disabled.
- The HTTP server is disabled.
- SNMP v1 and SNMP v2c are disabled. Only SNMP v3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients
- Generated RSA/DSA key pairs have a modulus length from 1024 to 2048 bits.
- SSH, SNMPv3, IPSec and SSL do not support DES, RC4, or MD5.

11 Physical Security Mechanism

FIPS 140-2 Security Level 2 Physical Security requirements mandate that a cryptographic module have an opaque enclosure with tamper-evident seals for doors or removable covers. HP Networking switches include both appliance and chassis models. The tamper-evident seals and opacity shields shall be installed for the module to operate in a FIPS Approved mode of

operation. All Networking switches need tamper-evident seals to meet the Physical Security requirements. Some models also need opacity shields (5820, 7506-V, and 7510).

The Crypto Officer is responsible for properly placing all tamper evident labels on a switch and is responsible for the securing and control of any unused seals and opacity shields. The Crypto Officer shall clean the module of any grease, dirt, or oil before applying the tamper-evident labels or opacity shields. The Crypto Officer is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident labels or opacity shields are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit:

All units use the same label kits:

| Label Kit – Description | Label Kit - Part Number |
|---|-------------------------|
| HP 12mm x 60mm Tamper-Evidence (30) Labels | JG585A |
| HP 12mm x 60mm Tamper-Evidence (100) Labels | JG586A |

The opacity kit for each product model is below:

5120-EI series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|---------------------|--|---------------------------|
| HP 5120-24G EI | HP 5500/5120 Gig-T EI Opacity Shield Kit | JG557A |
| HP 5120-48G EI | HP 5500/5120 Gig-T EI Opacity Shield Kit | JG557A |
| HP 5120-24G-PoE+ EI | HP 5500/5120 Gig-T PoE EI Opacity Shield Kit | JG559A |
| HP 5120-48G-PoE+ EI | HP 5500/5120 Gig-T PoE EI Opacity Shield Kit | JG559A |

5500 EI series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|---------------------|--|---------------------------|
| HP 5500-24G EI | HP 5500/5120 Gig-T EI Opacity Shield Kit | JG557A |
| HP 5500-24G-PoE+ EI | HP 5500/5120 Gig-T PoE EI Opacity Shield Kit | JG559A |
| HP 5500-24G-SFP EI | HP 5500-24G-SFP EI Opacity Shield Kit | JG558A |
| HP 5500-48G EI | HP 5500/5120 Gig-T EI Opacity Shield Kit | JG557A |
| HP 5500-48G-PoE+ EI | HP 5500/5120 Gig-T PoE EI Opacity Shield Kit | JG559A |

5800 series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|--------------------|---|---------------------------|
| HP 5800-24G | HP 5800-24G / -48G Opacity Shield Kit | JG563A |
| HP 5800-24G-PoE+ | HP 5800-24G / -48G PoE Opacity Shield Kit | JG560A |
| HP 5800-24G-SFP | HP 5800-24G-SFP Opacity Shield Kit | JG562A |
| HP 5800-48G | HP 5800-24G / -48G Opacity Shield Kit | JG563A |
| HP 5800-48G-PoE | HP 5800-24G / -48G PoE Opacity Shield Kit | JG560A |
| HP 5800-48G -2slot | HP 58xx 2-slot Switch Opacity Shield Kit | JG561A |

5820 series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|------------------|--|---------------------------|
| HP 5820-14XG-SFP | HP 58xx 2-slot Switch Opacity Shield Kit | JG561A |
| HP 5820-24XG-SFP | HP 5800-24XG-SFP+ Opacity Shield Kit | JG564A |

7500 series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|-----------|--|---------------------------|
| HP 7510 | HP 7510 Opacity Shield Kit | JG565A |
| HP 7506 | HP 7506 Opacity Shield Kit | JG566A |
| HP 7506V | HP 7506-V Opacity Shield Kit | JG567A |
| HP 7503 | HP 7503 Opacity Shield Kit | JG568A |
| HP 7502 | HP 75xx 1-slot Switch Opacity Shield Kit | JG569A |
| HP 7503-S | HP 75xx 1-slot Switch Opacity Shield Kit | JG569A |

9500 series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|----------|----------------------------|---------------------------|
| HP 9505 | HP 8805 Opacity Shield Kit | JG570A |
| HP 9508V | HP 8808 Opacity Shield Kit | JG571A |
| HP 9512 | HP 8812 Opacity Shield Kit | JG572A |

12500 series

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|----------|-----------------------------|---------------------------|
| HP 12508 | HP 12508 Opacity Shield Kit | JG574A |
| HP 12518 | HP 12518 Opacity Shield Kit | JG573A |

These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

Each modular switch is entirely encased by a thick steel chassis. Modular switches have one or two MPU slots and between two and eighteen slots for LPU. 12500 models have slots for switching fabric cards. On-board LAN connectors and console connectors are provided on the MPU board. Power cable connection and a power switch are provided on the power supplies. The individual modules that comprise the switch may be removed to allow access to the internal components of each module.

Any chassis slot that is not populated with a module must have a slot cover installed in order to operate in a FIPS compliant mode. The slot covers are included with each chassis, and additional slot covers may be ordered from HP.

Use the procedure described in FIPS enclosure install instruction to apply tamper evident labels and opacity shields to the switch.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

12 Mitigation of Other Attacks

The Security appliances do not claim to mitigate any attacks in a FIPS approved mode of operation.

13 Documentation References

13.1 Obtaining documentation

You can access the HP Networking products page: <http://h17007.www1.hp.com/us/en/> , where you can obtain the up-to-date documents of HP Routers and Switches, such as datasheet, installation manual, configuration guide, command reference , and so on.

13.2 Technical support

For technical or sales related question please refer to the contacts list on the HP website: <http://www.HP.com>.

The actual support website is:

<http://www8.hp.com/us/en/support-drivers.html>