

HP Network Switch

**Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version
K.15.09.0004**

**Models: 3800 with Software Version KA.15.09.0004
Security Target**

Version 3.3

Sept 22, 2012

Prepared For



Prepared By

CYGNACOM
SOLUTIONS

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Revision History

Date	Version	Author	Description
07/19/2012	3.0	Nancy Gow	Reworked for Maintenance Evaluation
07/26/2012	3.1	Nancy Gow	Updated from Vendor Comments
08/08/2012	3.2	Nancy Gow	Updated from NIAP Comments; Updated Crypto Table for FCP_COP.1
09/22/2012	3.3	Nancy Gow	Finalized

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table of Contents

- 1 Security Target Introduction..... 1**
- 1.1 Security Target Reference..... 1**
 - 1.1.1 References..... 1
- 1.2 TOE Reference 2**
- 1.3 TOE Overview 2**
 - 1.3.1 TOE Type 3
 - 1.3.2 Hardware/Firmware/Software Required by the TOE 3
- 1.4 TOE Description..... 4**
 - 1.4.1 Acronyms and Terminology 4
 - 1.4.2 Product Description..... 9
 - 1.4.2.1 HP Networking Switch Software 9
 - 1.4.2.2 HP Networking Switch Appliances..... 10
 - 1.4.2.3 ProVision ASIC..... 28
 - 1.4.2.4 User Interfaces 28
 - 1.4.2.5 Supporting Software..... 32
 - 1.4.3 Data..... 32
 - 1.4.4 Users 33
 - 1.4.5 Product Guidance..... 33
 - 1.4.6 Physical Scope of the TOE 34
 - 1.4.6.1 Included in the TOE 34
 - 1.4.6.2 TOE Operational Conditions 35
 - 1.4.6.3 Excluded from the TOE..... 36
 - 1.4.6.4 Operational Environment 36
 - 1.4.7 Logical Scope of the TOE 37
 - 1.4.7.1 Security Audit Functions 37
 - 1.4.7.2 Cryptographic Functions 37
 - 1.4.7.3 Information Flow Control Functions 37
 - 1.4.7.4 Identification and Authentication Functions 38
 - 1.4.7.5 Security Management Functions..... 38
 - 1.4.7.6 TOE Access Functions..... 38
 - 1.4.7.7 Protection of the TSF Functions..... 39
- 2 Conformance Claims..... 40**
 - 2.1 Common Criteria Conformance 40**
 - 2.2 Protection Profile Claim 40**
 - 2.3 Package Claim 40**
 - 2.4 Cryptographic Standard 40**
- 3 Security Problem Definition..... 41**
 - 3.1 Assumptions 41**
 - 3.2 Threats..... 41**

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- 3.3 Organizational Security Policies.....42
- 4 Security Objectives 43
 - 4.1 Security Objectives for the TOE43
 - 4.2 Security Objectives for the Operational Environment.....44
 - 4.3 Security Objectives Rationale.....45
- 5 Extended Components Definition 52
 - 5.1 FPT_ITC_EXP.1 Explicit: Partial Inter-TSF confidentiality during transmission ..52
 - 5.1.1 Class 52
 - 5.1.2 Family 52
 - 5.1.3 Family Behaviour..... 52
 - 5.1.4 Management 52
 - 5.1.5 Audit 52
 - 5.1.6 Definition 53
 - 5.1.7 Rationale 53
 - 5.2 FPT_TST_EXP.1 Explicit: TSF Self Testing.....53
 - 5.2.1 Class 53
 - 5.2.2 Family 53
 - 5.2.3 Family Behaviour..... 54
 - 5.2.4 Management 54
 - 5.2.5 Audit 54
 - 5.2.6 Definition 54
 - 5.2.7 Rationale 54
- 6 Security Requirements..... 56
 - 6.1 Security Functional Requirements for the TOE56
 - 6.1.1 Class FAU: Security Audit.....57
 - 6.1.1.1 FAU_GEN.1 Audit data generation57
 - 6.1.1.2 FAU_SAR.1 Audit review59
 - 6.1.1.3 FAU_STG.1 Protected audit trail storage60
 - 6.1.2 Class FCS: Cryptographic Support60
 - 6.1.2.1 FCS_CKM.1 Cryptographic key generation60
 - 6.1.2.2 FCS_CKM.4 Cryptographic key destruction61
 - 6.1.2.3 FCS_COP.1 Cryptographic operation.....61
 - 6.1.3 Class FDP: User Data Protection.....62
 - 6.1.3.1 FDP_IFC.1 (1) Subset information flow control (1)62
 - 6.1.3.2 FDP_IFF.1 (1) Simple security attributes (1)63
 - 6.1.3.3 FDP_IFC.1 (2) Subset information flow control (2)67
 - 6.1.3.4 FDP_IFF.1 (2) Simple security attributes (2)67
 - 6.1.3.5 FDP_IFC.1 (3) Subset information flow control (3)72
 - 6.1.3.6 FDP_IFF.1 (3) Simple security attributes (3)72
 - 6.1.3.7 FDP_IFC.1 (4) Subset information flow control (4)75
 - 6.1.3.8 FDP_IFF.1 (4) Simple security attributes (4)75
 - 6.1.3.9 FDP_IFC.1 (5) Subset information flow control (5)77
 - 6.1.3.10 FDP_IFF.1 (5) Simple security attributes (5)78
 - 6.1.4 Class FIA: Identification and Authentication83
 - 6.1.4.1 FIA_UAU.1 Timing of authentication83
 - 6.1.4.2 FIA_UAU.5 Multiple authentication mechanisms83
 - 6.1.4.3 FIA_UAU.7 Protected authentication feedback84

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

6.1.4.4	FIA_UID.1 Timing of identification.....	84
6.1.5	Class FMT: Security Management.....	84
6.1.5.1	FMT_MSA.1 Management of security attributes.....	84
6.1.5.2	FMT_MSA.3 Static attribute initialisation	85
6.1.5.3	FMT_MTD.1 Management of TSF data	85
6.1.5.4	FMT_SMF.1 Specification of Management Functions	88
6.1.5.5	FMT_SMR.1 Security roles	89
6.1.5.6	FMT_SMR.3 Assuming roles	89
6.1.6	Class FPT: Protection of the TSF	89
6.1.6.1	FPT_ITC_EXP.1 Explicit: Partial Inter-TSF confidentiality during transmission	89
6.1.6.2	FPT_TST_EXP.1 Explicit: TSF Self Testing	90
6.1.7	Class FTA: TOE access.....	90
6.1.7.1	FTA_TAB.1 Default TOE access banners	90
6.1.7.2	FTA_SSL.3 TSF-initiated termination	91
6.2	Security Assurance Requirements for the TOE.....	91
6.3	Security Requirements Rationale	91
6.3.1	Dependencies Satisfied	91
6.3.2	Functional Requirements	93
6.3.3	Assurance Rationale	99
7	TOE Summary Specification.....	100
7.1	IT Security Functions	100
7.1.1	Audit Functionality	101
7.1.1.1	SA-1: Audit Generation	101
7.1.1.2	SA-2: Audit Review	103
7.1.2	User I&A Functions	104
7.1.2.1	IA-1: Password Masking	104
7.1.2.2	IA-2: User Identification	105
7.1.2.3	IA-3: User Authentication	107
7.1.3	Information Flow Control	111
7.1.3.1	IFC-1 Connection-Rate Based Security Policy	111
7.1.3.2	IFC-2 Port Based Security Policy.....	113
7.1.3.3	IFC-3 Protocol Rate Limiting Security Policy	119
7.1.3.4	IFC-4 Port and Protocol Filtering Security Policy.....	122
7.1.3.5	IFC-5 ACL Filtering Security Policy.....	125
7.1.4	Security Management with Access Control	130
7.1.4.1	SM-1: Management Functions	130
7.1.4.2	SM-2: Management Security Roles	131
7.1.4.3	SM-3: Management Access Control	133
7.1.5	TOE Access	137
7.1.5.1	TA-1: Login Banner	137
7.1.5.2	TA-2 Inactivity Termination	138
7.1.6	Protection of TSF	139
7.1.6.1	TP-1: Cryptographic Support	139
7.1.6.2	TP-2: Self Testing.....	146

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table of Tables and Figures

Figure 1: Example Front Panel of a Model 3500yl HP Networking Switch	31
Figure 2: Example Front Panel of a Model 3800 HP Networking Switch	31
Figure 3: TOE Boundary Diagram	35
Figure 4: Format of an Event Log Entry	102
Figure 5: Example of an Event Log Display	103
Figure 6: Example of Masked Passwords during creation using CLI	104
Figure 7: Front Panel Buttons	105
Figure 8: Example of Configuring Manager and Operator Passwords	108
Figure 9: The Set Password Screen	108
Figure 10: Example of VACL Filter Application to IPv4 Traffic Entering the Switch	128
Figure 11: Example of RACL Filter Applications on Routed IPv4 Traffic	129
Figure 12: Example of Order of Application for Multiple ACLs on an Interface	130
Figure 13: Access Sequence for Privilege Levels	132
Figure 14: Example of CLI Result of the Login Banner Configuration	138
Figure 15: Example of Web Browser Interface Result of the Login Banner	138
Figure 16: Client Public Key SSH Authentication Model	141
Figure 17: Switch/User SSH Authentication	141
Figure 18: Switch/User SSL Authentication	143
Figure 19: Management Module Self test Boot Process Flow Chart	148
Table 1-1: References	1
Table 1-2: Product Acronyms/Terminology	4
Table 1-3: CC Acronyms/Terminology	9
Table 1-4: 8200zl Switch Specifications	11
Table 1-5: 5400zl Switch specifications	12
Table 1-6: 6600 Switch Specifications	15
Table 1-7: 6200yl Switch Specifications	19
Table 1-8: 3800 Switch Specifications	20
Table 1-9: 3500yl Switch Specifications	26
Table 3-1: Assumptions	41
Table 3-2: TOE Threats	41
Table 4-1: TOE Security Objectives	43
Table 4-2: Security Objectives for the Operational Environment	44
Table 4-3: Mapping of TOE Security Objectives to Threats/Policies	45
Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions	45
Table 4-5: All Threats to Security Countered	46
Table 4-6: All Assumptions and OSPs Upheld	50
Table 5-1: Extended Components	52
Table 6-1: Functional Components	56
Table 6-2: Auditable Events	57
Table 6-3: Cryptographic Support Parameters	60
Table 6-4: Cryptographic Algorithms	62
Table 6-5: Management of TSF data	85
Table 6-6: EAL2+ Assurance Components	91
Table 6-7: TOE Dependencies Satisfied	92
Table 6-8: Mapping of TOE SFRs to TOE Security Objectives	93
Table 6-9: All TOE Objectives Met by Security Functional Requirements	94
Table 7-1: Security Functional Requirements Mapped to Security Functions	100

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

<i>Table 7-2: Front Panel Button Actions</i>	<i>106</i>
<i>Table 7-3: Learning Modes</i>	<i>118</i>
<i>Table 7-4: Interface Options.....</i>	<i>126</i>
<i>Table 7-5: SSH Options</i>	<i>142</i>
<i>Table 7-6: Self Test Categories and Reactions</i>	<i>146</i>

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

1 Security Target Introduction

1.1 Security Target Reference

ST Title: HP Network Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04 Models: 3800 with Software Version KA.15.09.04 Security Target

Assurance level: EAL2 augmented with ALC_FLR.2

Protection Profile: None

1.1.1 References

Table 1-1 provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	ID
<i>HP Switch Software Access Security Guide (3500 switches, 3500yl switches, 3800 switches, 5400zl switches, 6200yl switches, 6600 switches, 8200zl switches) Software version K.15.09.04, June 2012</i>	[ASG]
<i>HP Switch Software Advanced Traffic Management Guide Software version K.15.09.04, June 2012</i>	[ATG]
<i>HP Switch Software Basic Operation Guide (HP 3500, HP 3800, HP 2520, HP 3500yl, HP 2620, HP 2520G, HP 5400zl, HP 2615, HP 6200yl, HP 2910, HP 6600, HP 2915, HP 8200zl), June 2012</i>	[BOP]
<i>Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3</i>	[CC]
<i>HP Switch Software Comware CLI Commands in ProVision (HP 3500, HP 3500yl, HP 5400zl, HP 6200yl, HP 6600, HP 8200zl) Software K.15.09.04, June 2012</i>	[CLI]
<i>HP Switch Software Event Log Message Reference Guide (HP 3500, HP 3800, HP 2520, HP 3500yl, HP 2620, HP 2520G, HP 5400zl, HP 2615, HP 6200yl, HP 2910a, HP 6600, HP 2915, HP 8200zl), June 2012</i>	[ELM]
<i>Hewlett-Packard Company\5400/8200 zl Switch Series Hardware Version: 5406 zl, 5412 zl, 8206 zl, and 8212 zl Firmware Version: K.15.07.0003 FIPS 140-2 Non-Proprietary Security Policy Version 1.0, July 16, 2012</i>	[FIPS]
<i>5998-3301 Switch Software IPv6 Configuration Guide, June 2012</i>	[IPv6]
<i>HP Switch Software Management and Configuration Guide (3500 switches, 3500yl switches, 3800 switches, 5400zl switches, 6200yl switches, 6600 switches, 8200zl switches) Software version K.15.09.04, June 2012</i>	[MCG]

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Reference Title	ID
<i>HP Switch Software Multicast and Routing Guide (3500 switches, 3500yl switches, 3800 switches, 5400zl switches, 6200yl switches, 6600 switches, 8200zl switches) Software version K.15.09.04, June 2012</i>	[MRG]
<i>Release Notes: Version K.15.09.04.0003 Software for the HP Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches, July 2012</i>	[RELNOTES]
<i>Software Feature Index for the HP 3500/3500yl/3800/5400zl/6200yl/6600/8200zl Switches, June 2012</i>	[SFI]

1.2 TOE Reference

TOE Identification: HP Network Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04 Models: 3800 with Software Version KA.15.09.04

TOE Vendor: Hewlett-Packard Company

1.3 TOE Overview

HP Networking Switches are intelligent network switches that provide a set of platform and software features that make them suited for enterprise edge, distribution/aggregation layer, and small core deployments. The TOE is the family of HP Networking Switch appliance models that run Version K.15.09.04 and KA.15.09.04 of the HP Networking software. The switch models (Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl) that run Software Version K.15.09.04 and the switch models (Models: 3800) that run Software Version KA.15.09.04 have a common ASIC architecture, unified software, and a unified set of easy-to-use management tools.

The TOE provides the following security functionality: generation of audit records for security relevant events and user review of these records; user identification and authentication and user login security; cryptographic support for data operations; information flow control; role-based access controlled security management features; protection of TSF data during transit; TSF self-testing; TOE access banners; and termination of a user session after a period of inactivity.

The HP Networking Switch's operating image base software is embedded in the switch appliances. The appliance hardware, the underlying operating systems, and third-party applications installed on the appliances provide support security functions of the TOE, and are included in the TOE.

This product was previously known as HP ProCurve Switches. Under an HP re-organization, HP has changed the reference to the TOE to be "HP Networking Switches". Titles to all Vendor user manuals have not been updated to reflect this change. Therefore, there are still references to ProCurve in user documentation and examples within the ST.

Note: HP Networking switch products based on the K.15.07.0003 code were submitted for FIPS 140-2 Level 2 certification using the Mocana cryptographic libraries. The cryptography in those products is now CAVP and CMVP certified. The HP Networking products based on the

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

K.15.09.04 and KA.15.09.04 are using the same Mocana cryptology libraries and implementation as the K.15.07.0003.

Note: It is not the intent of the evaluation to determine compliance to any IP standards mentioned in this ST. Testing will include specific filters identified for particular IP standards (i.e. ICMP filter). As a byproduct of the filter testing, certain aspects of the TOE's ability to parse IP packets and protocol formats will be confirmed. Protocol compliance is strictly by vendor assertion.

1.3.1 TOE Type

The HP Networking Switch is a series of scalable network switches used to build high-speed switched networks.

1.3.2 Hardware/Firmware/Software Required by the TOE

The HP Networking Switch's operating image base software Versions K.15.09.04 and KA.15.09.04 is embedded in the switch appliances. The appliance hardware, the underlying operating systems, and third-party applications installed on the appliances provide support security functions of the TOE, and are included in the TOE. As such, the operational environment of the TOE consists only of optional components.

- The TOE supports the optional use of an external SNTP server to provide reliable timestamps.
- The TOE supports the optional use of a Syslog Server and SNMP management server to send Event Log information to a centralized location. If this option is used, the environment is responsible for the secure storage of the Event Log information.
- The TOE supports the optional use of a standard SSL compatible Web Browser for use of its web-based management interface. CC requires using SSL option.
- The TOE supports remote management of its console interfaces. CC requires using SSH option. Therefore, the remote management station will require an SSH Client.
- The TOE supports the optional use of an external Syslog Server for event logging and debug messages
- The TOE supports the optional use of external RADIUS and TACACS+ authentication servers
- The TOE supports remote management of its MIB interfaces. CC requires using SNMPv3 with encrypted channel between the network management station and the TSF.

The TOE will be located in a location that provides physical security commensurate with the value of the data the TOE is switching, uninterruptible power, and the temperature control necessary for the reliable operation of the hardware.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

1.4 TOE Description

1.4.1 Acronyms and Terminology

Table 1-2: Product Acronyms/Terminology

Acronym/Term	Definition
3DES	Triple Data Encryption Algorithm (Triple DES) – a block cipher algorithm.
ACL	Access Control List - A list of permissions attached to an object.
AES	Advanced Encryption Standard - an encryption standard adopted by the U.S. government.
Aggregation Layer	The boundary between Layers 2 and 3 in the data center which therefore touches on product features at both the network and data-link layers of the OSI model.
ARP	Address Resolution Protocol - A method for finding a host's link layer (hardware) address when only its Internet Layer (IP) or some other Network Layer address is known.
ASCII	American Standard Code for Information Interchange - A character-encoding scheme based on the ordering of the English alphabet.
ASIC	Application-Specific Integrated Circuit - An integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use.
Blade	Blade servers are stripped down computer servers with a modular design optimized to minimize the use of physical space.
BPDU	Bridge Protocol Data Unit – A special data frame used to exchange information about bridge IDs and root path costs for a spanning tree.
CA	Certificate Authority - An entity that issues digital certificates for use by other parties.
CLI	Command Line Interface
Core Layer	The layer that is considered the backbone of a network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets.
DHCP	Dynamic Host Configuration Protocol - A network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
Distribution Layer	The layer that includes LAN-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs.
DNS	Domain Name System – A hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates information with domain names assigned to each of the participants.
DRAM	Dynamic Random Access Memory
DSA	Digital Signature Algorithm – A United States Federal Government standard or FIPS for digital signatures.
ECC	Error-Correcting Code
ECMP	Equal-Cost Multi-Path routing - A routing strategy where next-hop packet forwarding to a single destination can occur over multiple "best paths" which tie for top place in routing metric calculations.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Acronym/Term	Definition
Flash Memory	A non-volatile computer memory that can be electrically erased and reprogrammed.
FTP	File Transfer Protocol – A standard network protocol used to exchange and manipulate files over an Internet Protocol computer network
GARP	Generic Attribute Registration - A generic framework defined by the IEEE to provide bridges, switches, or other similar devices to be able to register and de-register attribute values, such as VLAN identifiers and multicast group membership across a large LAN.
GUI	Graphical User Interface
GVRP	GARP VLAN Registration Protocol
HMAC	Keyed-Hash Message Authentication Code - a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.
ICMP	Internet Control Message Protocol - One of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages
IDM	HP Networking Identity Driven Manager
IEEE 802.1X	An IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails.
IGMP	Internet Group Management Protocol - A communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.
IPv6	Internet Protocol version 6 (IPv6) - The next-generation Internet Protocol version designated as the successor to IPv4. It is an Internet Layer protocol for packet-switched internetworks.
Layer 2	The Data Link Layer of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model.
Layer 3	The Network Layer of the seven-layer OSI model of computer networking. The Network Layer is responsible for end-to-end (source to destination) packet delivery including routing through intermediate hosts, whereas the Data Link Layer is responsible for node-to-node (hop-to-hop) frame delivery on the same link.
LED	Light-Emitting Diode
MAC address	Media Access Control address – A unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification.
MD5	Message-Digest algorithm 5 - a widely used cryptographic hash function with a 128-bit hash value.
Meshing	The process of breaking up a domain into a series of sub-domains or cells
MIB	Management Information Base - A type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
MSTP	Multiple Spanning Tree Protocol - defines an extension to the RSTP protocol to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.
OSPF	Open Shortest Path First - a dynamic routing protocol for use in Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol and falls into the group of interior gateway protocols, operating within a single autonomous system (AS).

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Acronym/Term	Definition
PEM	Privacy Enhanced Mail - an early IETF proposal for securing email using public key cryptography.
PIM	Protocol-Independent Multicast - a family of multicast routing protocols that can provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet.
PIM-DM	PIM Dense Mode - implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present.
PIM-SM	PIM Sparse Mode -explicitly builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and optionally creates shortest-path trees per source
Q-in-Q	An Ethernet networking standard for Ethernet frame formats. Q-in-Q allows multiple VLAN headers to be inserted into a single frame
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service - a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. The RADIUS server is not part of the TOE, but can be optionally configured in the environment.
RC4	The most widely-used software stream cipher and is used in protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks).
RIJNDAEL	A collection of block ciphers.
RSA	Stands for Rivest, Shamir and Adleman who first publicly described it - an algorithm for public-key cryptography.
SCP	Secure Channel Protocol
SFTP	Secure File Transfer Protocol - a network protocol that provides file transfer and manipulation functionality over any reliable data stream.
SHA	Secure Hash Algorithm - a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.
SNMP	Simple Mail Transfer Protocol - an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
SNTP	Secure Network Time Protocol - a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
Spanning Tree	A spanning tree T of a connected, undirected graph G is a tree composed of all the vertices and some (or perhaps all) of the edges of G. Informally, a spanning tree of G is a selection of edges of G that form a tree spanning every vertex. That is, every vertex lies in the tree, but no cycles (or loops) are formed.
SSH	Secure Shell - a network protocol that allows data to be exchanged using a secure channel between two networked devices
SSL	Secure Sockets Layer - a cryptographic protocol that provides security for communications over networks such as the Internet.
Static Routing	A data communication concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network.
STP	Spanning Tree Protocol - a link layer network protocol that ensures a loop-free topology for any bridged LAN.
STP root bridge	The root bridge of the spanning tree is the bridge with the smallest (lowest) bridge ID.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Acronym/Term	Definition
TACACS+	Terminal Access Controller Access-Control System Plus - a protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services. A TACACS+ server is not part of the TOE, but can be optionally configured in the environment.
TCP	Transmission Control Protocol – a transport layer protocol (L4) that is one of the core protocols of the Internet protocol suite
Telnet	Telnet (teletype network) is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility.
TLS	Transport Layer Security the successor to Secure Sockets Layer (SSL),
TRUNK	Trunking is a concept by which a communications system can provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. A trunk is a single transmission channel between two points, each point being either the switching center or the node of a network. Network bonding (also known as port trunking) consists of aggregating multiple network interfaces into a single logical bonded interface that correspond to a single IP address.
UDP	User Datagram Protocol - a simple transport protocol used in the Internet
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol - a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet.
HP Networking SSH Terminology	
Enable Level	Manager privileges on the switch.
Key Pair	A pair of keys generated by the switch or an SSH client application. Each pair includes a public key, that can be read by anyone and a private key held internally in the switch or by a client.
Local password or username	A Manager-level or Operator-level password configured in the switch.
Login Level	Operator privileges on the switch.
PEM (Privacy Enhanced Mode)	Refers to an ASCII-formatted client public-key that has been encoded for portability and efficiency. SSHv2 client public-keys are typically stored in the PEM format.
Private Key	An internally generated key used in the authentication process. A private key generated by the switch is not accessible for viewing or copying. A private key generated by an SSH client application is typically stored in a file on the client device and, together with its public key counterpart, can be copied and stored on multiple devices.
Public Key	An internally generated counterpart to a private key. A device's public key is used to authenticate the device to other devices.
SSH Enabled	(1) A public/private key pair has been generated on the switch (generate ssh [dsa rsa]) and (2) SSH is enabled (ip ssh). (A key pair can be generated without enabling SSH, but SSH cannot be enabled without first generating a key pair.)
SSH Server	An HP Networking Switch with SSH enabled.
HP Networking SSL Terminology	
CA-Signed Certificate	A certificate verified by a third party certificate authority (CA). Authenticity of CA-Signed certificates can be verified by an audit trail leading to a trusted root certificate.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Acronym/Term	Definition
Digital Certificate	A certificate is an electronic “passport” that is used to establish the credentials of the subject to which the certificate was issued. Information contained within the certificate includes: name of the subject, serial number, date of validity, subject's public key, and the digital signature of the authority who issued the certificate. Certificates on HP Networking Switches conform to the X.509v3 standard, which defines the format of the certificate.
Key Pair	Public/private pair of RSA keys generated by switch, of which public portion makes up part of server host certificate and private portion is stored in switch flash (not user accessible).
Local password or username	A Manager-level or Operator-level password configured in the switch.
Manager Level	Manager privileges on the switch.
Operator Level	Operator privileges on the switch.
Root Certificate	A trusted certificate used by certificate authorities to sign certificates (CA-Signed Certificates) and used later on to verify that authenticity of those signed certificates. Trusted certificates are distributed as an integral part of most popular web clients. (See browser documentation for which root certificates are pre-installed).
Self-Signed Certificate	A certificate not verified by a third-party certificate authority (CA). Self-signed certificates provide a reduced level of security compared to a CA-signed certificate.
SSL Enabled	(1) A certificate key pair has been generated on the switch (web interface or CLI command: <code>crypto key generate cert [key size]</code>) (2) A certificate been generated on the switch (web interface or CLI command: <code>crypto host-cert generate self-signed [arg-list]</code>) and (3) SSL is enabled (web interface or CLI command: <code>web-management ssl</code>). (A key pair can be generated without enabling SSL, but SSL cannot be enabled without first generating a key pair.)
SSL Server	An HP Networking Switch with SSL enabled.
HP Networking Redundant Management Terminology	
Active Management Module	A management module that booted successfully and is actively managing the switch.
Failed Management Module	A management module that did not pass selftest and is not in standby mode.
Offline Management Module	A management module that is offline because redundancy is disabled.
Selftest	A test performed at boot to ensure the management module is functioning correctly. If the module fails selftest, it does not go into active or standby mode. If both modules fail selftest, the switch does not boot.
Standby Management Module	A management module that is ready to become the active management module if the active management module fails.
Switchover	When the other management module becomes the active management module.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table 1-3: CC Acronyms/Terminology

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.4.2 Product Description

HP Networking Switches are intelligent network switches that provide a set of platform and software features that make them suited for enterprise edge, distribution/aggregation layer, and small core deployments. The TOE is the family of HP Networking Switch appliance models that run Version K.15.09.04 of the HP Networking software. The switch models (Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl) that run Software Version K.15.09.04 have a common ASIC architecture, unified software, and a unified set of easy-to-use management tools. The 3800 switch models run the same software base; however it is compiled separately for the 3800 switch hardware and is designated as Software Version KA.15.09.04

All hardware, firmware, HP developed software and third-party software packages installed on the switch appliances are included in the TOE. TOE Components

The TOE includes all switch appliance models that run Version K.15.09.04 of the HP Networking software: 3500yl, 5400zl, 6200yl, 6600, 8200zl models and the 3800 appliance models that run Version KA.15.09.04, which are based on common platform architecture with common switch software and tools. These HP Networking Switches have been designed as a product family using the ProVision ASICs and software, providing consistency and scalability across the family.

1.4.2.1 HP Networking Switch Software

The Switch Models: 3500yl, 3800, 5400zl, 6200yl, 6600, 8200zl use the same software image base which includes the Intelligent Edge feature set standard. Although the 3800 Series switches use the exact same software as all other switches included in the TOE, the software is compiled separately with different libraries to work with the 3800 appliance hardware. Therefore, the 3800 Series software is designated as KA.15.09.04 rather than K.15.09.04.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Key security features provided by the software of the HP Networking Switch Models: 3500yl, 3800, 5400zl, 6200yl, 6600, and 8200zl models include:

- Audit Generation
 - Generation of Events that are stored on the switch and viewable through the CLI, Menu Interface, Web Interface mechanisms.
- Information Flow Control
 - Virus Throttle: connection Rate Filtering thwarts virus spreading by blocking routing from certain hosts exhibiting abnormal traffic behavior
 - ICMP throttling: defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic
 - Filtering capabilities: include Access Control Lists (ACLs), source port, multicast MAC address, and other protocol-based filtering capabilities
 - MAC address lockdown: maps a particular configured MAC address to a port and prevents any other unauthorized clients access to the network
 - MAC address lockout: prevents configured particular MAC addresses from connecting to the network
 - Source-port filtering: allows only specified ports to communicate with each other
 - DHCP protection: blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attack
 - Dynamic ARP protection: blocks Address Resolution Protocol (ARP) broadcast from unauthorized hosts, preventing eavesdropping or data theft of network data
 - Dynamic IP lockdown: works with DHCP protection to block traffic from unauthorized host, preventing IP source address spoofing
- Secure TOE Management:
 - All access methods—CLI, GUI, or MIB—are securely encrypted through SSHv2 and SSL and SNMPv3. (Management access via TELNET, HTTP, SNMP v1 and SNMP v2 is not allowed)
 - The TOE can be optionally configured to include an external authentication server
 - Security banner: displays customized security policy when users log in to the switch

1.4.2.2 HP Networking Switch Appliances

The primary differences among these switch families are hardware-related and include such aspects as port density and the number of power supplies and fans.

HP Network Switch

Models: 3500zl, 5400zl, 6200zl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

8200zl Series Appliances

The 8200zl Series appliances are a high-performance, highly available chassis switch platform that enables unified core-to-edge adaptive network solutions. It has platform and software high-availability features to provide system continuity and enhance network productivity.

Table 1-4: 8200zl Switch Specifications

8200zl Switch	
Included Accessories	1 8200zl Management Module (J9092A) 2 8200zl Fabric Module (J9093A) 1 8200zl System Support Module (J9095A) 1 HP Switch 8200zl Chassis/Fan Tray (J9091A)
Ports	12 open module slots Supports a maximum of 288 auto-sensing 10/100/1000 ports or 48 10-GbE ports or 288 mini-GBICs, or a combination
Power supplies	2 x required, 4 open power supply slots
Memory and processor	
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only. Optional 4-post cabinet rail available
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 480.3 million pps
Routing/Switching capacity	645.6 Gbps
Switch fabric speed	691.2 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries

5400zl Series Appliances

The 5400zl Series appliances consist of intelligent edge switches. The 5400zl models include 6-slot and 12-slot chassis and associated zl modules and bundles. The 5400zl models offer a variety of Gigabit interfaces, integrated PoE on all 10/100/1000Base-T ports, 10-GbE capability, and a choice of form factors.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table 1-5: 5400zl Switch specifications

5406zl Intelligent Edge Switch	
Ports	6 open module slots 1 RS-232C DB-9 console port Supports a maximum of 144 auto-sensing 10/100/1000 ports or 24 10-GbE ports or 144 mini-GBICs, or a combination
Power supplies	2 open power supply slots
Memory and processor	
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 240.2 million pps
Routing/Switching capacity	322.8 Gbps
Switch fabric speed	345.6 Gbps
Routing table size	10,000 entries
5406zl-48G Intelligent Edge Switch	
Included Accessories	2 Switch zl 24-Port 10/100/1000 PoE Module (J8702A) 1 Switch zl 875W Power Supply (J8712A)
Ports	4 open module slots 1 RS-232C DB-9 console port Supports a maximum of 144 auto-sensing 10/100/1000 ports or 16 10-GbE ports or 96 mini-GBICs, or a combination 48 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDI

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Power supplies	Includes: 1 x J8712A 1 open power supply slots
Memory and processor	
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 240.2 million pps
Routing/Switching capacity	322.8 Gbps
Switch fabric speed	345.6 Gbps
Routing table size	10,000 entries
5412zl Intelligent Edge Switch	
Ports	12 open module slots 1 RS-232C DB-9 console port Supports a maximum of 288 auto- sensing 10/100/1000 ports or 48 10- GbE ports or 288 mini-GBICs, or a combination
Power supplies	4 open power supply slots
Memory and processor	
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash Mb, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 480.3 million pps
Routing/Switching capacity	645.6 Gbps
Switch fabric speed	691.2 Gbps
Routing table size	10,000 entries

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

5412zl-96G Intelligent Edge Switch	
Included Accessories	4 Switch zl 24-Port 10/100/1000 PoE Module (J8702A) 2 Switch zl 875W Power Supply (J8712A)
Ports	8 open module slots 1 RS-232C DB-9 console port Supports a maximum of 288 auto-sensing 10/100/1000 ports or 32 10-GbE ports or 192 mini-GBICs, or a combination 96 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only
Power supplies	Includes: 2 x J8712A 2 open power supply slots
Memory and processor	
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash Mb, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64)
10 Gbps Latency	<2.1 μ s (FIFO 64)
Throughput	Up to 480.3 million pps
Routing/Switching capacity	645.6 Gbps
Switch fabric speed	691.2 Gbps
Routing table size	10,000 entries

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Fixed Port Switches:

6600 Series Appliances

The 6600 Series appliances consist of data center server edge switches. The 6600 models includes 1U 10/100/1000Base-T and 10-GbE SFP+ stackables enhanced for server edge connectivity with front-to-back cooling, redundant hot-swappable power, and redundant hot-swappable fans.

Table 1-6: 6600 Switch Specifications

6600-24G Switch	
Ports	20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) 1 RS-232C DB-9 console port
Power supplies	includes: 1 x J9269A 2 open power supply slots
Fan Tray	Includes 1 x J9271A 1 Fan tray slot Fan tray supports N+N fans for added redundancy.
Memory and processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash; 256 MB compact flash, 256 MB DDR SDRAM; packet buffer size: 18 MB QDR SDRAM total (for all 1-GbE ports)
Mounting	Telco rack: Mounts in an EIA-standard 19-in. 2-post telco rack or equipment cabinet; horizontal surface mounting only. Rack kit: Rack rails are required for mounting in HP 10000 Series 4-post racks.
Performance	

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 35.7 million pps
Routing/Switching capacity	48 Gbps
Switch fabric speed	48 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries
6600-24G-4XG Switch	
Ports	<p>20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) 4 SFP+ 10-GbE ports Duplex: full only 1 RS-232C DB-9 console port</p>
Power supplies	<p>includes: 1 x J9269A 2 open power supply slots</p>
Fan Tray	<p>Includes 1 x J9271A 1 Fan tray slot Fan tray supports N+N fans for added redundancy.</p>
Memory and processor	<p>Freescale PowerPC 8540 @ 666 MHz, 4 MB flash; 256 MB compact flash, 256 MB DDR SDRAM; packet buffer size: 36 MB QDR SDRAM total (18 MB for all 1-GbE ports, 18 MB for all 10-GbE ports)</p>
Mounting	<p>Telco rack: Mounts in an EIA-standard 19-in. 2-post telco rack or equipment cabinet; horizontal surface mounting only. Rack kit: Rack rails are required for mounting in HP 10000 Series 4-post racks.</p>
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 75.7 million pps
Routing/Switching capacity	101.8 Gbps
Switch fabric speed	105.6 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries
6600-24XG Switch	
Ports	24 SFP+ 10-GbE ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: full only 1 RJ-45 serial console port
Power supplies	includes: 1 x J9269A 2 open power supply slots
Fan Tray	Includes 1 x J9271A 1 Fan tray slot Fan tray supports N+N fans for added redundancy
Memory and processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash; 1 GB compact flash, 256 MB DDR SDRAM; packet buffer size: 108 MB QDR SDRAM total (for all 10-GbE ports)
Mounting	Telco rack: Mounts in an EIA-standard 19-in. 2-post telco rack or equipment cabinet; horizontal surface mounting only. Rack kit: Rack rails are required for mounting in HP 10000 Series 4-post racks.
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 240.2 million pps
Routing/Switching capacity	322.8 Gbps
Switch fabric speed	345.6 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries
6600-48G Switch	

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Ports	44 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) 1 RJ-45 console port
Power supplies	Includes: 1 x J9269A 2 open power supply slots
Fan Tray	Includes 1 x J9271A 1 Fan tray slot Fan tray supports N+N fans for added redundancy.
Memory and processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash; 1 GB compact flash, 256 MB DDR SDRAM; packet buffer size: 36 MB QDR SDRAM total (for all 1-GbE ports)
Mounting	Mounts in an EIA-standard 19 in. 2-point telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 71.4 million pps
Routing/Switching capacity	96 Gbps
Switch fabric speed	96 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries
6600-48G-4XG Switch	
Ports	48 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 4 SFP+ 10-GbE ports (IEEE 802.3ak Type 10Gbase-CX4) Duplex: full only 1 RJ-45 console port

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Power supplies	Includes: 1 x J9269A 2 open power supply slots
Fan Tray	Includes 1 x J9271A 1 Fan tray slot Fan tray supports N+N fans for added redundancy.
Memory and processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash; 1 GB compact flash, 256 MB DDR SDRAM; packet buffer size: 72 MB QDR SDRAM total (36 MB for all 1-GbE ports, 36 MB for all 10- GbE ports)
Mounting	Mounts in an EIA-standard 19 in. 2- point telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 130.9 million pps
Routing/Switching capacity	176 Gbps
Switch fabric speed	176 Gbps
Routing table size	10,000 entries
MAC address table size	64,000 entries

6200yl Appliances

The 6200yl-24G-mGBIC appliance is an advanced Layer 3 stackable in 1U height. It has 24 mini- GBIC slots and an expansion slot for an optional 4-port 10-GbE module. Designed to be deployed as an aggregator of traffic from the edge to the core of the network, this model supports a variety of Gigabit mini-GBICs, such as SX, LX, LH, and 1000Base-T.

Table 1-7: 6200yl Switch Specifications

Switch 6200yl-24G-mGBIC	
Ports	1 open module slot 24 open mini-GBIC (SFP) slots Supports a maximum of 4 10-GbE ports, with optional module
Processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only.
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 75.7 million pps
Routing/Switching capacity	101.8 Gbps
Switch fabric speed	105.6 Gbps
Routing table size	10,000 entries

3800 Series Appliances

The HP 3800 Series is a family of fully managed Gigabit Ethernet switches. There are a total of nine switch models—a 24-port switch, a 48-port switch, a 24-port PoE+ switch, a 48-port PoE+ switch with either SFP+ or 10GBASE-T uplinks, and a 24-port SFP switch with 2 SFP+ uplinks

Table 1-8: 3800 Switch Specifications

HP 3800-24G-PoE+-2SFP+ Switch (J9573A)	
Included Accessories	1 HP X312 1000W 100-240VAC to 54VDC Power Supply (J9580A) 1 HP 3800 Switch Fan Tray (J9582A)
Ports	24 RJ-45 autosensing 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9580A (HP X312 1000W 100-240VAC to 54VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 18 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only.
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	65.4 million pps (64-byte packets)
Switching capacity	88 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-48G-PoE+-4SFP+ Switch (J9574A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X312 1000W 100-240VAC to 54VDC Power Supply (J9580A)
Ports	48 RJ-45 autosensing 10/100/1000 PoE+ ports

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

	(IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9580A (HP X312 1000W 100-240VAC to 54VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-24G-2SFP+ Switch (J9575A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)
Ports	24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-48G-4SFP+ Switch (J9576A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)
Ports	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-48G-4SFP+ Switch (J9576A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)
Ports	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

	includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-24G-2XG Switch (J9585A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)
Ports	24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 RJ-45 10-GbE ports IEEE 802.3an-2006 Type 10GBASE-T; Duplex: full only 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 18 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	65.4 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-48G-4XG Switch (J9586A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Ports	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 RJ-45 10-GbE ports IEEE 802.3an-2006 Type 10GBASE-T; Duplex: full only 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM GB; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-24G-PoE+-2XG Switch (J9587A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X312 1000W 100-240VAC to 54VDC Power Supply (J9580A)
Ports	24 RJ-45 autosensing 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 RJ-45 10-GbE ports IEEE 802.3an-2006 Type 10GBASE-T; Duplex: full only 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9580A (HP X312 1000W 100-240VAC to 54VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 18 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	65.4 million pps (64-byte packets)
Switching capacity	88 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-48G-PoE+-4XG Switch (J9588A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X312 1000W 100-240VAC to 54VDC Power Supply (J9580A)
Ports	48 RJ-45 autosensing 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 RJ-45 10-GbE ports IEEE 802.3an-2006 Type 10GBASE-T; Duplex: full only 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot
Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9580A (HP X312 1000W 100-240VAC to 54VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 36 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	130.9 million pps (64-byte packets)
Switching capacity	176 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries
HP 3800-24SFP-2SFP+ Switch (J9584A)	
Included Accessories	1 HP 3800 Switch Fan Tray (J9582A) 1 HP X311 400W 100-240VAC to 12VDC Power Supply (J9581A)
Ports	24 SFP 100/1000 Mbps ports (IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 100BASE-TX: half or full; 1000BASE-T: full only 2 fixed 1000/10000 SFP+ ports 1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 Stacking module slot

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Power supplies	2 power supply slots 1 minimum power supply required includes: 1 x J9581A (HP X311 400W 100-240VAC to 12VDC Power Supply)
Memory and processor	HP ProVision ASIC/ARM @ 350 MHz; Freescale PowerPC @ 1200 MHz, 4 GB flash, 2 GB SDRAM; packet buffer size: 18 MB dynamic
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	< 2.8 μ s (LIFO 64-byte packets)
10 Gbps Latency	< 1.9 μ s (LIFO 64-byte packets)
Throughput	65.4 million pps (64-byte packets)
Switching capacity	88 Gbps
Routing table size	10,000 entries
MAC address table size	65,500 entries

3500yl Series Appliances

The 3500yl Series appliances consist of intelligent edge switches. The 3500yl models include 24-port and 48-port stackables. The 3500yl models offer a variety of Gigabit interfaces, integrated PoE on all 10/100/1000Base-T ports, 10-GbE capability, and a choice of form factors.

Table 1-9: 3500yl Switch Specifications

Switch 3500yl-24G-PWR Intelligent Edge	
Ports	1 open module slot 20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 1 RS-232C DB-9 console port 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) with PoE or an open mini-GBIC slot (for use with mini-GBIC transceivers) Supports a maximum of 4 10-GbE ports
Memory and processor	
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Stackable memory and processor: Freescale PowerPC 8540 @ 666 MHz,

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

	4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 75.7 million pps
Routing/Switching capacity	101.8 Gbps
Switch fabric speed	105.6 Gbps
Routing table size	10,000 entries
Switch 3500yl-48G-PWR Intelligent Edge	
Ports	1 open module slot 44 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) Media type: Auto-MDIX Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 1 RS-232C DB-9 console port 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) with PoE or an open mini-GBIC slot (for use with mini-GBIC transceivers) Supports a maximum of 4 10-GbE ports
Memory and processor	
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Stackable memory and processor: Freescale PowerPC 8540 @ 666 MHz, 4 MB flash Mb, 128 MB compact flash, 256 MB DDR SDRAM
Mounting	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Performance	
1000 Mb Latency	<3.7 μ s (FIFO 64-byte packets)
10 Gbps Latency	<2.1 μ s (FIFO 64-byte packets)
Throughput	Up to 111.5 million pps
Routing/Switching capacity	149.8 Gbps

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Switch fabric speed	153.6 Gbps
Routing table size	10,000 entries

1.4.2.3 ProVision ASIC

The HP Networking ProVision™ ASIC is the fourth generation of HP Networking's network chipsets. A key component of the HP Networking Switches, the highly integrated ProVision ASIC has built-in wirespeed intelligence, a unified set of configuration management tools and is scalable across a number of products. The ProVision ASIC is designed to operate continuously and withstand error conditions and malicious network attacks. The HP Networking Switches use a combination of software and ProVision ASIC functionality to verify all the data packets sent to the CPU. Excessive packets from malicious attacks or network mis-configuration can be identified and demoted to lower-priority queues before they overwhelm and shut down the CPU and the switch. In addition, the ProVision ASIC contains processes such as end-to-end data checking, embedded RAM error correction, and ECC on an external DRAM. These processes ensure the integrity of the traffic as it passes through the switch, protecting the traffic from environmental elements.

1.4.2.4 User Interfaces

The TOE includes a number of management interfaces that enable users to reconfigure the switch and to monitor switch status and performance. The TOE offers the following interfaces:

CLI

The CLI is a command line interface offering the full set of switch commands through the VT-100/ANSI console built into the switch. Support for SSH (in-band) access to the menu functionality is also included. The CLI provides the following functionality:

- Provides access to the complete set of the switch configuration, performance, and diagnostic features.
- Offers out-of-band access (through the RS-232 connection) or SSH (inband) access.
- Enables quick, detailed system configuration and management access to system operators and administrators experienced in command prompt interfaces.
- Provides help at each level for determining available options and variables.
- other distinct interfaces can be initiated from CLIs: Menu interface & Test mode interface.

Menu Interface

The Menu interface is initialized by executing a CLI after successful authentication. Therefore, the same out-of-band and in-band accessibility to the CLIs applies to this

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

interface. The Menu interface provides management access to a menu-driven subset of switch configuration and performance features:

- IP addressing
- System information
- VLANs and GVRP
- Local passwords
- Port Security
- SNMP communities
- Port and Static Trunk Group
- Time protocols
- Spanning Tree

The Menu interface also provides access for:

- Setup screen
- Switch and port statistic and counter displays
- Event Log display
- Reboots
- Switch and port status displays
- Download software image to switch

Testmode Interface

This interface is for maintenance and troubleshooting only and is not included in the scope of the evaluation.

- Undocumented functionality that should only be initiated when directed by HP support.
- Must have a legitimate administrator account on the switch

Web Interface

The Web interface is a switch interface offering status information and a subset of switch commands through a standard web browser (such as Mozilla Firefox or Microsoft Internet Explorer). The Web interface provides the following functionality:

- Easy access to the switch from anywhere on the network
- Familiar browser interface--locations of window objects consistent with commonly used browsers, uses mouse clicking for navigation, no terminal setup

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Many features have all their fields in one screen so users can view all values at once
- More visual cues, using colors, status bars, device icons, and other graphical objects instead of relying solely on alphanumeric values
- Display of acceptable ranges of values available in configuration list boxes

Front-Panel Access

In addition to the user interfaces listed above, the TOE provides a physical interface that is available to users on the front panel of the switch appliance. This physical interface includes:

- A set of switch, expansion module and indicator LEDs to indicate proper operation of the switch
- The LED Mode select button which allows the user to step from one LED view mode to the next.
- The Reset Button used to reset the switch while it is powered on. This action clears any temporary error conditions that may have occurred and executes the switch self test. It is also used when restoring the switch factory default configuration.
- The Clear Button used to delete any switch console access passwords and also to restore the switch to its factory configuration.
- The Console port (serial port) used to directly connect to the switch and requires authentication when used. This port cannot be turned off.

Because the Front-Panel is available to anyone with physical access to the switch, the switch must be physically protected from unauthorized users. The TOE provides the Manager with the ability to lock the Front-panel to prevent access as well. Figures 1 and 2 show examples of the Front Panel interface for the HP Networking Switches.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

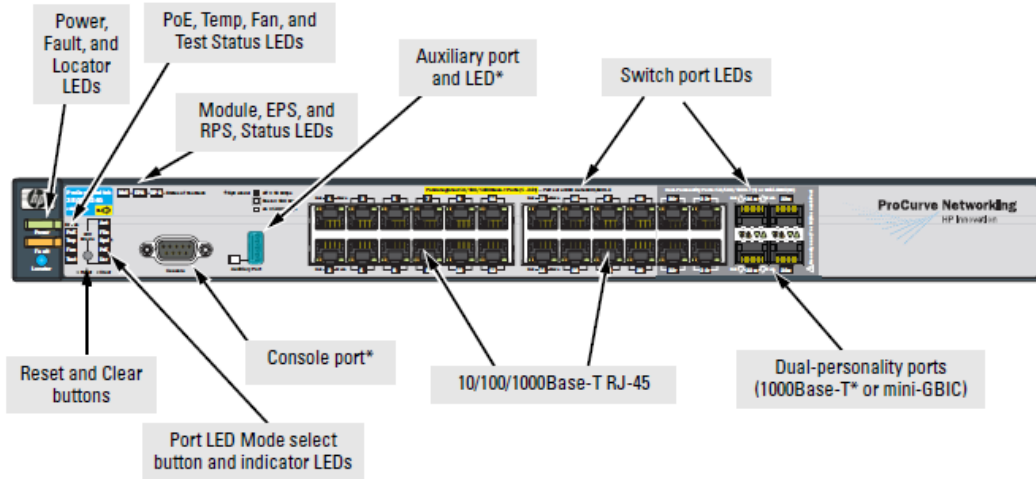


Figure 1: Example Front Panel of a Model 3500yl HP Networking Switch

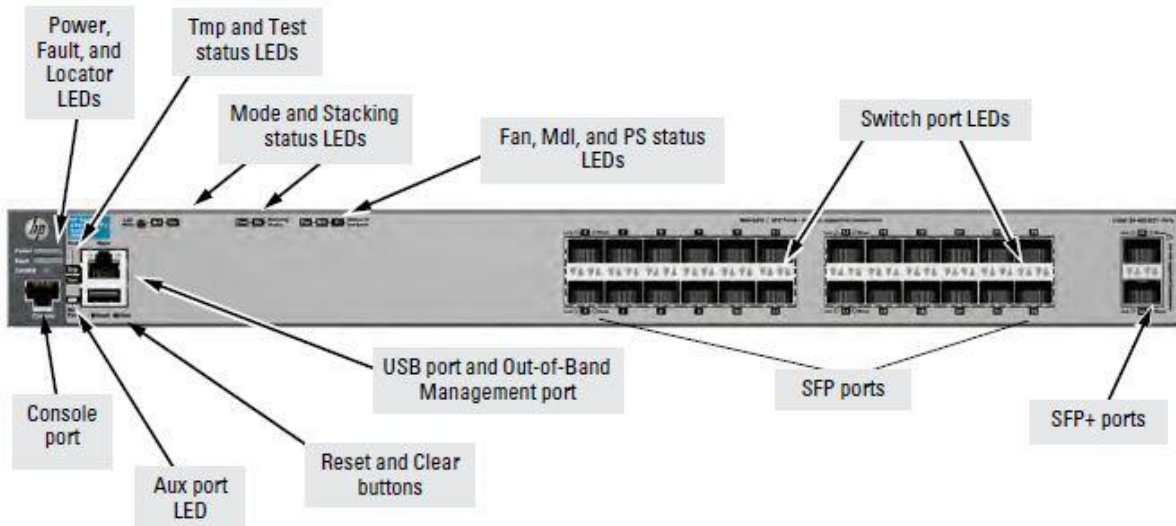


Figure 2: Example Front Panel of a Model 3800 HP Networking Switch

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Network Management Station Interface

There is the ability for an administrator to manage the TOE via a network management station using SNMP. The TOE allows the following subset of the authentication MIB objects to be remotely changed via SNMP:

- number of primary and secondary login and enable attempts
- TACACS+ server configuration and status
- RADIUS server configuration
- selected 802.1X settings
- key management subsystem chain configuration
- key management subsystem key configuration
- Open Shortest Path First (OSPF) interface authentication configuration
- local switch operator and manager usernames and passwords

This interface should be disabled if not being used. CC evaluated configuration requires that SNMP v1 & v2 be disabled and SNMPv3 with encryption enabled. The network management station (NMS) and the NMS's user interface are NOT in the scope of the TOE.

1.4.2.5 Supporting Software

The switch appliances also include an HP internally developed web-server to support the web-based administrative interface.

In addition to HP developed software, the TOE also includes third-party software installed on the switch appliances that support the security functionality of the TOE. These third-party software packages include:

- Operating System: Green Hills Integrity v5.0.11
- Mocana 5.3.1 for SSH and SSL

HP is responsible for any patches or fixes related to these products. The customer cannot update these software packages via patches from the original third-party vendor.

1.4.3 Data

All data managed by the TOE can be categorized as TSF data and includes data used to configure, manage, and operate the TOE such as: user account data and parameters set by the administrators to configure the security of the TOE and Audit (Event) data produced by the TOE for security significant events.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

The TOE does not store or provide mechanisms for end-users (network clients) to create user data. All user data is passed through or blocked by the TOE based on the customized security policies.

1.4.4 Users

All direct users (managers and operators) of the TOE have access to management functions and can therefore be considered administrators. End-users (network clients) do not have access to the TOE's management functionality.

The TOE supports two management roles for the Menu and Web interfaces: Operator and Manager. Each role allows access to a set of privileges (management functions and data). The CLI provides two additional levels of privilege: Global Configuration and Contextual Configuration. The user roles are hierarchical where the operator is least privileged and Manager with Contextual Configuration is most privileged. Managers have access to both the Global Configuration and Contextual Configuration

A user must be successfully identified and authenticated before being allowed access to any functionality of the CLI, Web or Menu interfaces.

In addition to the interfaces specified above, the TOE provides a physical interface on the front panel of the switch (console port). Therefore the switch must be physically protected to prevent unauthorized users from accessing the switch appliance. This console port can be configured with a password.

1.4.5 Product Guidance

The CC version of all HP Networking Switch documentation, including Release Notes covering recently added features, is available at the HP Networking Web site:
<http://www.hp.com/networking/support>.

The two publications listed below are printed and shipped with the switch.

- Read Me First—Provides software update information, product notes, and other information.
- Installation and Getting Started Guide—Explains how to prepare for and perform the physical installation and connect the switch to the network.

The CC version of each of the publications listed below is available in PDF format on the HP Networking Web site, as described above.

- Management and Configuration Guide—Describes how to configure, manage, and monitor basic switch operation.
- Advanced Traffic Management Guide—Explains how to configure traffic management features such as VLANs, MSTP, QoS, and Meshing.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Multicast and Routing Guide—Explains how to configure IGMP, PIM, IP routing, and VRRP features.
- Access Security Guide—Explains how to configure access security features and user authentication on the switch.
- IPv6 Configuration Guide—Describes the IPv6 protocol operations that are supported on the switch.
- Command Line Interface Reference Guide—Provides a comprehensive description of CLI commands, syntax, and operations.
- Event Log Message Reference Guide—Provides a comprehensive description of event log messages.
- Release Notes—Describes new features, fixes, and enhancements that become available between revisions of the main product guide.
- Common Criteria for HP Networking Switches Read Me First — Defines the operational assumptions and configuration conditions required for the TOE to be installed in the CC Evaluated configuration.

1.4.6 Physical Scope of the TOE

1.4.6.1 *Included in the TOE*

The TOE consists of the entire HP Networking Switch, Software Version K.15.09.04 and KA.15.09.04 as available commercially from the Vendor. The TOE consists of all hardware, firmware, HP developed software, Intelligent Edge features, and third party software installed upon the switch appliance. A simple example of an operational installation of the HP Networking Switch 3500yl-24G is shown below:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

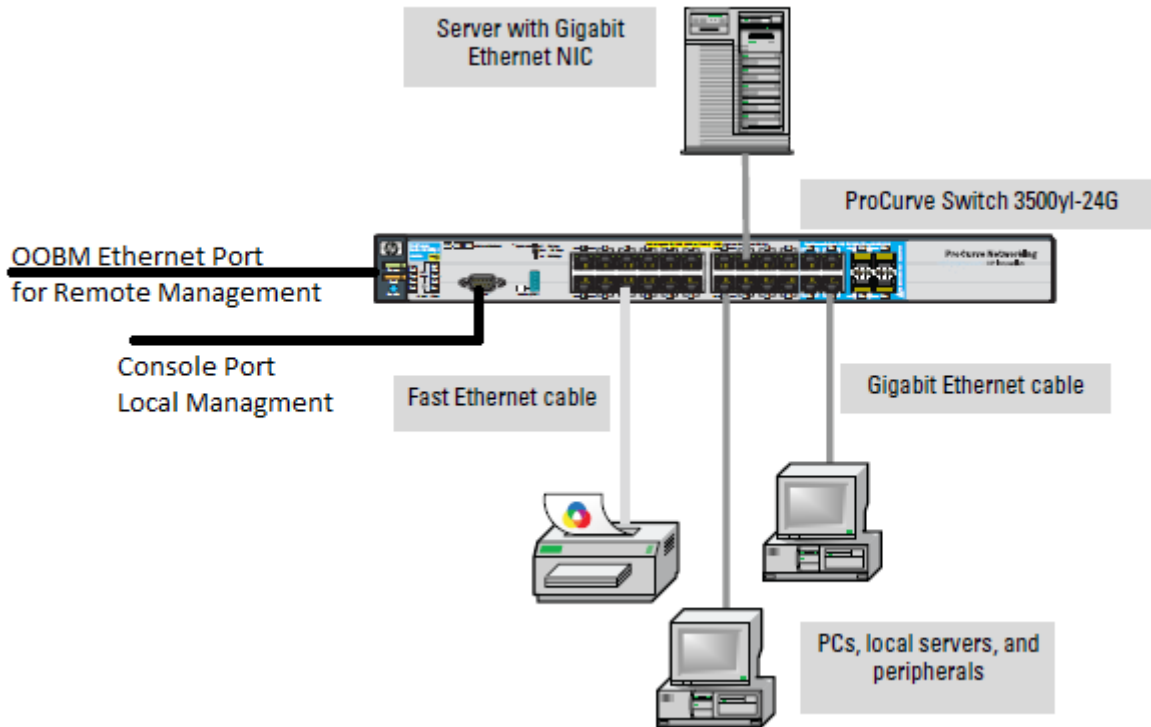


Figure 3: TOE Boundary Diagram

1.4.6.2 TOE Operational Conditions

- TELNET for CLI and Menu Interfaces must be disabled and SSH must be used.
- HTTP Web access for management using a standard web browser connection must be disabled.
- HTTPS must be enabled for Web access management
- TFTP client and server must be disabled.
- Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP) should be enabled.
- SNMP v2 and v1 must be disabled.
- SNMP v3 with encryption should be enabled if remote SNMP Management is used.
- Replace the default community name ("public") with a non-default community name.
- Manager and Operator access levels must have a password assigned.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Full individual user identification and authentication can only be achieved if the switch is configured so that identification and authentication are handled via an external authentication server (RADIUS or TACACS+) or certificates.
- The console inactivity timer must be configured to a nonzero value.
- There are two recessed buttons on the front-panel of the switch: “password clear” and “factory reset.” Both must be disabled to fully secure the device.
- The switch includes a USB port to receive a flash drive for deploying, troubleshooting, backing up configurations, or updating switches. This port should be disabled when not in use and temporarily enabled when needed.
- DO NOT disable Password-Recovery option

1.4.6.3 Excluded from the TOE

The following are not included in the TOE:

- PCM and PCM+ are network management applications that can optionally be used to manage and monitor HP Networking Switches via SNMP from an MS Windows-based workstation/server. A copy of PCM and PCM+ (trial-version) is included on the CD-ROM that comes with the TOE. However, these are separate HP products that will not be evaluated.
- Testmode Interface (accessed via CLI) which is only used for maintenance and troubleshooting.

1.4.6.4 Operational Environment

The following are optional operational environment components that are not included in the TOE:

- External authentication server(s) (RADIUS, TACACS+)
- External SNTP Server (Time Sync Server)
- External Syslog Server
- External SNMP Server
- External client software to support 802.1X
- DNS Server
- SSL compatible Web Browser for use of web-based management interface (Web Interface support)
- SSH Client on host used to support remote management of console interfaces (CLI and Menu Interface)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- External Network Management Station and software used for remote management of MIB attributes over SNMPv3
- Connected networks and assets

1.4.7 Logical Scope of the TOE

The security functionality provided by the IT Environment is also described in Section 4.2 Security Objectives for the Operational Environment. Section 7 TOE Summary Specification gives detailed information on how these security functions that make up the logical scope of the TOE are implemented.

The TOE provides the following security functionality:

1.4.7.1 Security Audit Functions

The TOE records security relevant event data in an Event Log. The audit records in the Event Log serve as a tool to isolate and troubleshoot problems. The audit trail is stored on the switch and is accessible via the protected management functional interfaces. The TOE is able to protect the Event Log from unauthorized deletion or modification. TOE users can view the audit records via the Menu Interface and the CLI.

The Security Audit Functions may optionally depend on an SNTP Server in the operational environment to provide reliable timestamps for the audit records. Event Log records and debugging messages can be optionally sent to an external Syslog Server or sent via SNMP trap as new events are generated. There is the ability to export the entire event log via TFTP and SFTP for off TOE storage and review.

1.4.7.2 Cryptographic Functions

The TOE provides cryptographic support for SSH communications; SSL data transport; SNMP messaging and authentication support; hashing of passwords; secure communications with an external authentication server (RADIUS primarily used for network and mac authentication) or TACACS management access); and for MAC Authentication (port based access control). HP Networking switch products based on the K.15.07.0003 code were submitted for FIPS 140-2 Level 2 certification using the Mocana cryptographic libraries. The cryptography in those products is now CAVP and CMVP certified. The HP Networking products based on the K.15.09.04 and KA.15.09.04 software are using the same Mocana cryptology libraries and implementation as the K.15.07.0003.

1.4.7.3 Information Flow Control Functions

The TOE performs user data protection through information flow control. Only legitimate external IT entities are granted access to pass information through the TOE or to the TOE. Traffic is allowed or blocked through the use of rate filtering, ICMP throttling, protocol-based

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

filtering, source-port filtering and dynamic ARP protection. Traffic can be blocked from unauthorized DHCP servers, configured MAC addresses, configured IP addresses and source-ports and through the use of access control lists.

1.4.7.4 Identification and Authentication Functions

The TOE enforces password based authentication before allowing access to the command line, menu and web-based management interfaces. The TOE also allows the use of an optional external authentication server (RADIUS or TACACS+) for TOE user identification and authentication.

The TOE enhances user login security by masking passwords during entry on user login.

Identification and Authentication functionality may optionally depend on the operational environment by use of an external authentication server.

1.4.7.5 Security Management Functions

The TOE supports role-based access to the administrative interfaces and management functions. The TOE provides the following management interfaces: a Command Line Interface (CLI), a Menu Interface, a Web-Based interface, and a physical interface available on the front panel of the switch appliance, and a MIB interface.

The TOE supports management of the security attributes that are used for information flow control.

The TOE supports administrative security roles: Manager, Operator, Global Configuration (CLI only), Context Configuration (CLI only). Each role provides a set of privileges to access the management functions of the web, menu, and command line interfaces.

The Security Management functionality depends on the remote management console using SSH for accessing the console interfaces (CLI or Menu Interface) or a SSL enabled web browser for use of the Web interface.

Functionality is provided for the disabling/locking the Front Panel Interface and the USB interface to prevent unauthorized physical tampering.

In order to use the MIB interface the TOE requires the use of an operational environmentally supplied Network Management Station, which is not in scope, with SNMPv3 enabled.

1.4.7.6 TOE Access Functions

The TOE displays a banner regarding unauthorized use of the TOE before establishing a user session. The TOE will also terminate a user's session after an administrator configured period of inactivity.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

1.4.7.7 Protection of the TSF Functions

The TOE in conjunction with the operational environment protects TSF data from unauthorized disclosure when transmitted between itself and trusted external IT entities.

The TOE is also capable of self-testing during initial start-up and reboot to detect security failures.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant. The assurance requirements contained in this ST meet EAL2 augmented with ALC_FLR.2 as defined in the Common Criteria version 3.1 R3. The HP Networking product meets the requirements of this ST and provides for a basic level of robustness. Under the *Arrangements on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*, only CC requirements at or below EAL2 are mutually recognized.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST claims conformance to EAL2 augmented with ALC_FLR.2.

2.4 Cryptographic Standard

HP Networking switch products based on the K.15.07.0003 code were submitted for FIPS 140-2 Level 2 certification using the Mocana cryptographic libraries. The cryptography in those products is now CAVP and CMVP certified. The HP Networking products based on the K.15.09.04 (and KA.15.09.04) software are using the same Mocana cryptology libraries and implementation as the K.15.07.0003.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

3 Security Problem Definition

This section defines the expected TOE security environment in terms of the threats, security assumptions, and the security policies that must be followed for the high robustness TOE.

3.1 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are as follows:

Table 3-1: Assumptions

Item	Assumption ID	Assumption Description
1	A.Admin	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
2	A.Manage	It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.
3	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.
4	A.Physical	It is assumed that the TOE hardware and software critical to the security policy enforcement will be protected from unauthorized physical modification.
5	A.ProtectPwd	It is assumed that users will protect their authentication data.

3.2 Threats

The TOE addresses the following threats:

Table 3-2: TOE Threats

Item	Threat ID	Threat Description
1	T.Intercept	An attacker may gain access to and/or modify TSF data while it is being transmitted between the switch and external operational environment servers used for remote management and I&A.
2	T.Masquerade	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources via the TOE interfaces.
3	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Threat ID	Threat Description
4	T.NoPrivilege	A user may gain access to management functions or TSF data for which they are not authorized by the assigned role resulting in the TSF data being compromised.
5	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.
6	T.RateBased	An External IT Entity may exhaust service resources of the TOE or systems by passing information flows through the TOE.
7	T.AddressSpoof	An External IT Entity may illegitimately gain access to networks through the TOE by spoofing source IP address.
8	T.UndesiredAccess	An External IT Entity may send impermissible information through the TOE, which results in the exploitation of resources.
9	T.ICMPDoS	An External IT Entity may exhaust service resources of the TOE or systems through ICMP denial-of-service attacks.
10	T.InsecureState	The TOE may be placed in an insecure state as a result of an erroneous initialization, halt, reconfiguration or restart, or as a result of an unsuccessful recovery from a system failure or discontinuity.

3.3 Organizational Security Policies

Item	OSP ID	Policy Description
1	P.Password	TOE users will be instructed to choose secure passwords that meet the Password Policy defined in the user guidance documentation.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.Access	The TOE will allow access to the protected management functions and TSF data only to authorized users with the appropriate security roles via the TOE interfaces.
2	O.AssumingRoles	The TOE will require that an explicit request along with a password must be given to assume (change to a) the Manager role from an Operator Role.
3	O.AuditGeneration	The TOE will provide the capability to create records of security-relevant events and associate these events with the process which caused the event.
4	O.AuditProtect	The TOE will protect its own audit trail from unauthorized modification and deletion.
5	O.AuditReview	The TOE will provide the capability for review of the audit information to authorized users via the protected TOE management interfaces.
6	O.Banner	The TOE will display an access banner prior/during Login process. This banner will be customizable by the administrators.
7	O.CryptoSupport	The TOE will provide cryptographic functions for protecting TSF data during transmission to another IT trusted product.
8	O.InactivityTermination	The TOE will terminate a session due to an administratively defined period of inactivity.
9	O.Manage	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.
10	O.ProtectAuth	The TOE will provide protected authentication feedback by masking password as input with asterisks.
11	O.RobustTOEAccess	The TOE will provide a native I&A mechanism and the functionality to invoke optional external I&A mechanisms to control the user's logical access to the protected interfaces of the TOE.
12	O.SelfTest	The TOE will automatically run a series of self tests during boot to ensure the proper operation of the hardware and software modules of the TOE.
13	O.TransProtect	The TOE must protect all TSF data from unauthorized disclosure during transmission to the external authentication server by ensuring that a secure channel is used.
14	O.UndesiredAccess	The TOE must control unauthorized information flow between internal and external networks based on security policies.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	TOE Objective	Description
15	O.RateBased	The TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DoS and DDoS attacks, and authorized users who may overuse resources.
16	O.ProtocolFiltering	The TOE must be able to perform protocol-based filtering, which includes forwarding, dropping, automatic throttling of ICMP, or automatic throttling of all protocol traffic.
17	O.ProtectComm	The TOE must protect all TSF data from unauthorized disclosure during transmission to the remote user management terminal by ensuring that a secure channel is used.

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Table 4-2: Security Objectives for the Operational Environment

Item	Environment Objective	Description
1	OE.AuthService*	The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.
2	OE.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.
3	OE.Operations	The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.
4	OE.PasswordSelect	Those responsible for the management of the TOE will only allow users to establish passwords according to requirements in the user guidance.
5	OE.Person	Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.
6	OE.Physical	The Operational Environment will provide physical protection for the TOE.
7	OE.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
8	OE.ProtectComm	The remote user management terminal will protect all TSF data from unauthorized disclosure during transmission to the TSF by establishing a secure channel with the TOE.
9	OE.Time	The Operational Environment will provide reliable time stamps.
10	OE.TransProtect	The external authentication server will protect all TSF data from unauthorized disclosure during transmission to the TSF by establishing a secure channel with the TOE.

**Note: OE.AuthService is only applicable to the TOE if is configured to use an external authentication service. (I.e. RADIUS Server)*

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

4.3 Security Objectives Rationale

Table 4-3: Mapping of TOE Security Objectives to Threats/Policies

Item	TOE Objective	Threat
1	O.Access	T.NoPrivilege
2	O.AssumingRoles	T.NoPrivilege
3	O.AuditGeneration	T.Undetect
4	O.AuditProtection	T.Undetect
5	O.AuditReview	T.Undetect
6	O.Banner	T.NoPrivilege
7	O.CryptoSupport	T.Intercept
8	O.InactivityTermination	T.Masquerade
9	O.Manage	T.Mismanage
10	O.ProtectAuth	T.Masquerade
11	O.RobustTOEAccess	T.Masquerade
12	O.SelfTest	T.InsecureState
13	O.TransProtect	T.Intercept
14	O.UndesiredAccess	T.AddressSpoof T.UndesiredAccess
15	O.RateBased	T.RateBased
16	O.ProtocolFiltering	T.ICMPDoS
17	O.ProtectComm	T.Intercept

Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions

Item	Environment Objective	Threat/Policy/Assumption
1	OE.AuthService	T.Masquerade
2	OE.NoUntrusted	A.NoUntrusted
3	OE.Operations	A.Manage
4	OE.PasswordSelect	P.Password
5	OE.Person	A.Admin
6	OE.Physical	A.Physical
7	OE.ProtectAuth	A.ProtectPwd
8	OE.ProtectComm	T.Intercept
9	OE.Time	T.Undetect
10	OE.TransProtect	T.Intercept

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table 4-5: All Threats to Security Countered

Item	Threat ID	Objective	Rationale
1	T.Intercept An attacker may gain access to and/or modify TSF data while it is being transmitted between TOE components.	O.TransProtect The TOE must protect all TSF data from unauthorized disclosure during transmission to the external authentication server by ensuring that a secure channel is used.	This objective contributes to mitigating this threat by ensuring that the TOE uses secure TSF data transmission practices that have been established in conjunction with the Operational Environment to protect data between the external authentication servers.
		O.ProtectComm The TOE must protect all TSF data from unauthorized disclosure during transmission to the remote user management terminal by ensuring that a secure channel is used.	This objective contributes to mitigating this threat by ensuring that the TOE uses secure TSF data transmission practices that have been established, in conjunction with the Operational Environment, to protect TSF data between the remote user management terminal and the TOE.
		O.CryptoSupport The TOE will provide cryptographic functions for protecting TSF data during transmission to another IT trusted product.	This objective contributes to mitigating this threat by ensuring that the TOE will provide the mechanisms encrypt the data being transmitted
		OE.TransProtect The external authentication server will protect all TSF data from unauthorized disclosure during transmission to the TSF by establishing a secure channel with the TOE.	This objective also contributes to mitigating this threat by ensuring that the Operational Environment will support the use of secure TSF Data transmission between the external authentication servers and the TOE.
		OE.ProtectComm The remote user management terminal will protect all TSF data from unauthorized disclosure during transmission to the TSF by establishing a secure channel with the TOE.	This objective also contributes to mitigating this threat by ensuring that the Operational Environment will support the use of secure TSF Data transmission between the remote user management terminal and the TOE.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Threat ID	Objective	Rationale
2	T.Masquerade A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.	O.ProtectAuth The TOE will provide protected authentication feedback.	This objective mitigates the threat by providing the masking of a user's password to keep it from being overseen by another.
		O.RobustTOEAccess The TOE will provide a native I&A mechanism and the functionality to invoke optional external I&A mechanisms to control the user's logical access to the protected interfaces of the TOE.	This objective mitigates this threat by controlling the logical access to the TOE and its resources through the login process. By constraining how authorized users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective allows the TOE to correctly interpret information used during the authentication process so that it can make the correct decisions when identifying and authenticating users.
		O.InactivityTermination The TOE will terminate a session due to an administratively defined period of inactivity.	This objective mitigates the threat by ending idle sessions which if left open could allow someone to gain access and masquerade as the legitimate user.
		OE.AuthService The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.	This objective mitigates the threat by allowing the use of an external user authentication service that is invoked by the TSF to support a Robust TOE Access control policy.
3	T.Mismanage Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	O.Manage The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.	This objective mitigates this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, it provides administrators with the capability to configure and operate the TOE via a CLI, Menu Interface, and web interface.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Threat ID	Objective	Rationale
4	T.NoPrivilege A user may gain access to management functions or TSF data for which they are not authorized by the assigned role resulting in the TSF data being compromised.	O.Access The TOE will allow access to the protected management functions and TSF data only to authorized users with the appropriate security roles via the TOE interfaces.	This objective mitigates this threat by limiting the functions a user can perform and the data they can access via the TOE interfaces through the use of user security roles and permissions.
		O.AssumingRoles The TOE will require that an explicit request along with a password must be given to assume (change to a) the Manager role from an Operator Role.	This objective also mitigates the threat by providing the requirement that to assume a new privileged role (Operator to Manager) that a specific request and password is required.
		O.Banner The TOE will display an access banner prior/during Login process. This banner will be customizable by the administrators.	This objective also mitigates the threat by providing a warning banner with an appropriate warning notifying the person attempting to gain access about the system.
5	T.Undetect Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.	O.AuditGeneration The TOE will provide the capability to create records of security-relevant events and associate these events with the process which caused the event.	This objective mitigates this threat by providing the TOE with an audit logging function that keeps records of security significant events.
		O.AuditReview The TOE will provide the capability for review of the audit information to authorized users via the protected TOE management interfaces.	This objective also mitigates this threat by providing administrative personnel with the capability to efficiently review the audit information and spot a security breach.
		O.AuditProtect The TOE will protect its own audit trail from unauthorized modification and deletion..	This objective also mitigates this threat by ensuring an accurate audit trail by preventing unauthorized deletion and/or modification.
		OE.Time The Operational Environment will provide reliable time stamps.	This objective contributes to mitigating the threat by providing each audit record with an accurate time stamp for ease of viewing and piecing together timelines.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Threat ID	Objective	Rationale
6	T.RateBased An External IT Entity may exhaust service resources of the TOE or systems by passing information flows through the TOE.	O.RateBased The TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DoS and DDoS attacks, and authorized users who may overuse resources.	This threat is mitigated by O.RateBased, which requires that the TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must also be able to serve as a rate based controller and police both malicious users who attempt to flood your network with DoS and DDoS attacks, and authorized users who may overuse resources.
7	T.AddressSpoof An External IT Entity may illegitimately gain access to networks through the TOE by spoofing source IP address.	O.UndesiredAccess The TOE must control unauthorized information flow between internal and external networks based on security policies.	This threat is mitigated by O.UndesiredAccess, which requires that the TOE must control unauthorized information flow from the external network to the internal network based on security policies. This objective also prevents information flows of from spoofed IP addresses arriving at physical ports, which do not match the address range, associated with the ports.
8	T.UndesiredAccess An External IT Entity may send impermissible information through the TOE, which results in the exploitation of resources.	O.UndesiredAccess The TOE must control unauthorized information flow between internal and external networks based on security policies.	This threat is mitigated by O.UndesiredAccess, which requires that the TOE must control unauthorized information flow from the external network to the internal network based on security policies.
9	T.ICMPDoS An External IT Entity may exhaust service resources of the TOE or systems through ICMP denial-of-service attacks.	O.ProtocolFiltering The TOE must be able to perform protocol-based filtering, which includes forwarding, dropping, automatic throttling of ICMP, or automatic throttling of all protocol traffic.	This threat is mitigated by O.ProtocolFiltering which requires that the TOE must filter the information flows through the TOE by protocol to prevent malicious intruders flooding the system resources via ICMP DoS attacks

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Threat ID	Objective	Rationale
10	T.InsecureState The TOE may be placed in an insecure state as a result of an erroneous initialization, halt, reconfiguration or restart, or as a result of an unsuccessful recovery from a system failure or discontinuity.	O.SelfTest The TOE will automatically run a series of self tests during boot to ensure the proper operation of the hardware and software modules of the TOE.	The TOE will automatically run a series of self tests during boot to ensure the proper operation of the hardware and software modules of the TOE thus mitigating a possibility of the TOE being put into an unknown or insecure state.

Table 4-6: All Assumptions and OSPs Upheld

Item	Assumption ID	Objective	Rationale
1	A.Admin It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.	OE.Person Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.	This objective provides for competent personnel to administer the TOE.
2	A.Manage It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.	OE.Operations The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.	This objective ensures that all TOE users follow the guidance for secure installation, configuration and operation procedures.
3	A.NoUntrusted It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.	OE.NoUntrusted The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.	This objective provides for the protection of the TOE from untrusted software and users.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Assumption ID	Objective	Rationale
4	A.Physical It is assumed that the TOE hardware and software critical to the security policy enforcement will be protected from unauthorized physical modification.	OE.Physical The Operational Environment will provide physical protection for the TOE.	This objective provides for the physical protection of the TOE. As the TOE is an appliance this protection would include both hardware and software.
5	A.ProtectPwd It is assumed that users will protect their authentication data.	OE.ProtectAuth Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.	This objective provides for all TOE users protecting their authentication data.
6	P.Password TOE users will be instructed to choose secure passwords that meet the Password Policy defined in the user guidance documentation.	OE.PasswordSelect Those responsible for the management of the TOE will only allow users to establish passwords according to requirements in the user guidance.	This objective reinforces the concept that the Password policy is administratively enforced via the recommended procedure described in the administrative guidance. This policy applies to both Native password capabilities and external password authentication capabilities.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding “_EXP” in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FPT_ITC_EXP.1	Explicit: Partial Intra-TSF confidentiality during transmission
2	FPT_TST_EXP.1	Explicit: TSF Self Testing

5.1 *FPT_ITC_EXP.1 Explicit: Partial Inter-TSF confidentiality during transmission*

5.1.1 Class

FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.2 Family

Inter-TSF confidentiality during transmission (FPT_ITC)

5.1.3 Family Behaviour

This family provides requirements that address protection of TSF data when it is transferred between separate parts of a TOE across an internal channel.

5.1.4 Management

The following actions could be considered for the management functions in FMT:

- None anticipated

5.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of the trusted channel functions

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Minimal: Identification of the initiator and target of failed trusted channel functions
- Basic: All attempted uses of the trusted channel functions
- Basic: Identification of the initiator and target of all trusted channel functions

5.1.6 Definition

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITC_EXP.1.1 The TSF shall protect all TSF data transmitted from the TSF to the external ***[assignment: list external IT devices that require trusted communication with the TOE]*** from unauthorized disclosure during transmission.

5.1.7 Rationale

FPT_ITC_EXP.1 is modeled closely on the standard component FPT_ITC.1: Inter-TSF confidentiality during transmission. There are no trusted channel SFRs that exist for establishing a trusted channel between TOE and external (OE) devices. For this particular TOE there are 2 different trusted channels required. One is for TOE to remote management terminals (browser) and another is for TOE to external authentication servers (which the TOE invokes when configured). This explicitly stated SFR is not a requirement for any internal TOE communications. ITC was selected as it was closest to what was required.

5.2 ***FPT_TST_EXP.1 Explicit: TSF Self Testing***

5.2.1 Class

FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.2 Family

TSF Self Testing (FPT_TST)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

5.2.3 Family Behaviour

The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. Examples are interfaces to enforcement functions, and sample arithmetical operations on critical parts of the TOE. These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. The actions to be taken by the TOE as the result of self testing are defined in other families.

5.2.4 Management

The following actions could be considered for the management functions in FMT:

- management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
- management of the time interval if appropriate.

5.2.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Execution of the TSF self tests and the results of the tests.

5.2.6 Definition

Hierarchical to: No other components.

Dependencies: No other components.

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests [**selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and [assignment: conditions under which self test should occur]**] to demonstrate the correct operation of the TSF.

FPT_TST_EXP.1.2 Upon detection of a test failure the TSF [**assignment: list events and conditions**]

5.2.7 Rationale

FPT_TST_EXP.1 is modeled closely on the standard component FPT_TST.1: TSF testing. It was needed to be defined as an extended component because the standard component did not take into accounts the failure procedures and verification of correct operation. The original also included the ability to check the integrity of the stored TSF executable code as a whole. The

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

extended SFR only includes the particular Management modules and not the product as a whole.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

- iteration: allows a component to be used more than once with varying operations;
- assignment: allows the specification of parameters;
- selection: allows the specification of one or more items from a list; and
- refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text]***.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified the inclusion of a suffix on the name of the element consisting of a parenthesized number indicating the iteration number. For example, fdp_ifc.2.1 (1) indicates the first iteration of fdp_ifc.2.1 while fdp_ifc.2.1 (2) indicates the second iteration.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: with italicized text*
- *Extended components* defined in Section 5 have been denoted with the suffix "_EXP" following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5, and summarized in Table 6-1 below.

Table 6-1: Functional Components

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit Review
3	FAU_STG.1	Protected audit trail storage

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	SFR ID	SFR Title
4	FCS_CKM.1	Cryptographic key generation
5	FCS_CKM.4	Cryptographic key destruction
6	FCS_COP.1	Cryptographic operation
7	FDP_IFC.1 (1)	Subset information flow control (1)
8	FDP_IFF.1 (1)	Simple security attributes (1)
9	FDP_IFC.1 (2)	Subset information flow control (2)
10	FDP_IFF.1 (2)	Simple security attributes (2)
11	FDP_IFC.1 (3)	Subset information flow control (3)
12	FDP_IFF.1 (3)	Simple security attributes (3)
13	FDP_IFC.1 (4)	Subset information flow control (4)
14	FDP_IFF.1 (4)	Simple security attributes (4)
15	FDP_IFC.1 (5)	Subset information flow control (5)
16	FDP_IFF.1 (5)	Simple security attributes (5)
17	FIA_UAU.1	Timing of authentication
18	FIA_UAU.5	Multiple authentication mechanisms
19	FIA_UAU.7	Protected authentication feedback
20	FIA_UID.1	Timing of identification
21	FMT_MSA.1	Management of security attributes
22	FMT_MSA.3	Static attribute initialisation
23	FMT_MTD.1	Management of TSF data
24	FMT_SMF.1	Specification of Management Functions
25	FMT_SMR.1	Security roles
26	FMT_SMR.3	Assuming roles
27	FPT_ITC_EXP.1	Explicit: Partial Inter-TSF confidentiality during transmission
28	FPT_TST_EXP.1	Explicit: TSF Self Testing
29	FTA_TAB.1	Default TOE access banners
30	FTA_SSL.3	TSF-initiated termination

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a. Start-up and shutdown of the audit functions;
- b. All auditable events for the **[not specified]** level of audit; and
- c. **[list of auditable events]**

Table 6-2: Auditable Events

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	SFR ID	Audit Event	Example(s)
1	FAU_GEN.1	System Startup System Shutdown	System booted/reboot
			<mod-num> is shutting down
			System boot/reboot to Radius Server
2	FAU_SAR.1	none	N/A
3	FAU_STG.1	none	N/A
4	FCS_CKM.1	Success and failure of the activity.	<num-bits>-bits <rsa dsa> client public key <installed removed> <manager operator> access. (key-comment)
			SSL HTTP startup failed: no certificate present
5	FCS_CKM.4	Success and failure of the activity.	SSH host key zeroized
6	FCS_COP.1	none	N/A
7	FDP_IFC (1)	none	N/A
8	FDP_IFF (1)	Decisions to permit requested information flows.	A port with the specified IP address has been throttled after detecting a relatively high number of connection-rate attempts from a host.
9	FDP_IFC (2)	none	N/A
10	FDP_IFF (2)	Decisions to permit requested information flows.	ICMP traffic exceeded configured limit on port <portname>
11	FDP_IFC (3)	none	N/A
12	FDP_IFF (3)	Decisions to permit requested information flows.	<mod-num>: <mac-addr> detected on port <port-num> (A locked out MAC address attempted to transmit a packet into the network from the specified module.)
13	FDP_IFC.1 (4)	none	N/A
14	FDP_IFF.1 (4)	Decisions to permit requested information flows.	<mod-num>: Client packet destined to untrusted port <port-num> Dropped (A unicast packet with a destination address on an untrusted port was received from a DHCP client and was dropped.)
15	FDP_IFC.1 (5)	none	N/A
16	FDP_IFF.1 (5)	Decisions to permit requested information flows.	<mod-num>: Client packet destined to untrusted port <port-num> Dropped (A Dropped packet based on ACL match or implicit deny)
17	FIA_UAU.1	Unsuccessful use of the user authentication mechanism, including the user identity provided.	Invalid user name/password on <session-type> session
18	FIA_UAU.5	Unsuccessful use of the authentication mechanism.	A remote login attempt failed
			Can't reach external authentication server
19	FIA_UAU.7	none	N/A

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	SFR ID	Audit Event	Example(s)
20	FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided.	Invalid user name/password on <session-type> session
21	FMT_MSA.1	Errors in modifications to the values of security attributes.	Inconsistent <mac-addr> config with <config-type> - <config-type>
22	FMT_MSA.3	Errors in modifications to the initial values of security attributes.	Bad reconfiguration request <request>
23	FMT_MTD.1	All modifications to the values of TSF data.	IP address <ip-addr>/<mask> configured on vlan-id <vlan-id>
			Port <port-num> is in Half Duplex - set to Individual
24	FMT_SMF.1	Use of the management functions.	Resetting Mgmt Module <mod-num>
			Password(s) removed via clear button
25	FMT_SMR.1	none	N/A
26	FMT_SMR.3	none	N/A
27	FPT_ITC_EXP.1	Failure of the trusted channel functions.	SSL HTTP server disabled
			The SSH session was aborted.
			SNMP Security access violation from <src-ip-addr>
28	FPT_TST_EXP.1	Execution of the TSF self tests and the results of the tests.	Boot-up selftest failed
			<mod-num>: Self-test failed <msg-txt>
29	FTA_TAB.1	none	N/A
30	FTA_SSL.3	none	N/A

J.

Application Note: The product doesn't have a specific event for startup and shutdown of the audit function. However, since the audit is started with the TOE it is met via the audit event for the Startup and Shutdown of the TOE.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[Severity Code, optional event number, and description of the event]**.

Application Note: Subject Identity is fulfilled using the System Module field. The System Module is the internal module (such as "ports:" for port manager) that generated a log entry.

6.1.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FAU_SAR.1.1 The TSF shall provide **[Operators and Managers]** with the capability to read **[all audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **[prevent]** unauthorised modifications to the stored audit records in the audit trail.

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[listed in Column 1 of Table 6-3]** and specified cryptographic key sizes **[listed in Column 2 of Table 6-3]** that meet the following: **[SSL version 3, TLS version 1.0, TLS version 1.1, TLS version 1.2, or SSHv2]**.

Table 6-3: Cryptographic Support Parameters

Key Type	Format	Key Size	Description (standard)
RSA	PEM or ASCII format	1024, 1536, 2048, 3072, 4096 bits	Facilitate Key transfer over SSH connection. (SSHv2)
RSA key pair	ASCII	1024, 1536, 2048, 3072, 4096 bits	For use in generating the server certificates used in SSL support. (SSLv3, TLSv1.0, 1.1, 1.2)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Application Note: SSL and SSH in the switches is based on the Mocana software toolkit

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[zeroization]** that meets the following: **[SSL version 3, TLS version 1.0, TLS version 1.1, TLS version 1.2, or SSHv2]**.

6.1.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **[operations listed in Column 4 Table 6-4]** accordance with a specified cryptographic algorithm **[listed in Column 2 of 4 Table 6-4]** and cryptographic key sizes **[listed in Column 2 of 4 Table 6-4]** that meet the following: **[SSL version 3, TLS version 1.0, TLS version 1.1, TLS version 1.2,, or SSHv2]**.

HP Network Switch

Models: 3500zl, 5400zl, 6200zl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table 6-4: Cryptographic Algorithms

Algorithm Type	Algorithm	Use
Cipher support for SSH	AES128-CBC 3DES-CBC AES192-CBC AES256-CBC RIJNDAEL-CBC@LYSATOR.LIU.SE ¹ AES128-CTR AES192-CTR AES256-CTR	encrypt/decrypt operations
Cipher support for SSL	AES256_SHA AES128_SHA	encrypt/decrypt operations
Cipher support for SNMP version 3	AES128-CFB	encrypt/decrypt operations
hashing	SHA1 MD5 SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	Passwords SNMP V3 Authentication support, TACACS+, RADIUS
HMAC (Keyed-Hash Message Authentication Code)	HMAC-SHA1 HMAC-MD5 HMAC-SHA1-96 HMAC-MD5-96 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	MAC Authentication (MAC-Auth) method grants access to a secure network by authenticating devices for access to the network. Port based access control

6.1.3 Class FDP: User Data Protection

6.1.3.1 FDP_IFC.1 (1) Subset information flow control (1)

Hierarchical to: No other components

Dependencies: FDP_IFF.1

¹ An AES-CBC cipher developed at Lysator (an academic computer society located at [Linköping University](http://www.lysator.liu.se) in Linköping, Sweden)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FDP_IFC.1.1 (1) The TSF shall enforce the **[Connection-Rate Based Security Policy]** on:

[

a) Subject:

Source Subjects: Source Client

Destination Subjects: Target Client(s)

b) Information:

Network traffic between Source subjects and Destination Subjects

c) Operation:

PERMIT information flow

DENY information flow

].

6.1.3.2 FDP_IFF.1 (1) Simple security attributes (1)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 (1) The TSF shall enforce the **[Connection-Rate Based Security Policy]** based on the types of subject and information security attributes:

[

a) Subject security attributes:

Source Subjects: Presumed IP address of the Source Client

Destination Subject: Presumed IP address of the Target Client(s)

b) Information security attributes:

- **Number of Connection requests per Source Client per inbound servicing Switch Port**
- **Protocol of network traffic**
- **Connection-rate ACL**
 - **Individual Host IP entry**
 - **Group of Hosts entry**
 - **Subnet entry**

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- *UDP/TCP Criteria*
- *Connection Request Threshold Rate Attributes (Global Sensitivity Setting)*
 - *LOW (mean of 54 routed destinations in less than .1 seconds)*
 - *MEDIUM (mean of 37 routed destinations in less than 1 second)*
 - *HIGH (mean of 22 routed destinations in less than 1 second)*
 - *AGGRESSIVE (mean of 15 routed destinations in less than 1 second)*
- *Penalty Time (Global Sensitivity Setting)*
 - *LOW : between 0 and less than 30 seconds*
 - *MEDIUM: between 30 and less than 60 seconds*
 - *HIGH: between 60 and less than 90 seconds*
 - *AGGRESSIVE between 90 and 120 seconds*

]

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

[

IF

(Protocol Check)

1. Network traffic is NOT IPv6 network traffic

AND

(Connection rate filtering enabled check)

2. Connection rate filtering has been turned on for the specific port

AND

(Connection-Rate ACL Check)

3. ACL does NOT exist

THEN skip this check (go to 4)

ELSE (ACL exists):

IF Source Client IP address and UDP/TCP Criteria is NOT contained in Connection Rate ACL THEN skip this check (go to 4)

ELSE

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

IF Source Client IP address is contained as an individually identified host and Connection Rate ACL entry is set to “filter”

OR

If Source Client IP address is contained within an identified group of hosts and Connection Rate ACL entry is set to “filter”

OR

If Source Client IP address is contained within an identified subnet and Connection Rate ACL entry is set to “filter”

AND

(Sensitivity Threshold Check)

4. The Total Number of Connection requests per Source Client per inbound servicing Switch Port made during a period of time does NOT exceed the rate bound by the Global Sensitivity Setting:

- ***LOW : mean of 54 routed destinations in less than .1 seconds***
- ***MEDIUM : mean of 37 routed destinations in less than 1 second***
- ***HIGH : mean of 22 routed destinations in less than 1 second***
- ***AGGRESSIVE : mean of 15 routed destinations in less than 1 second***

THEN

PERMIT information flow to Target Client(s)

].

FDP_IFF.1.3 (1) The TSF shall enforce the ***[Manager configured responses***

IF The Total Number of Connection requests per Source Client per servicing Switch Port made during a period of time does exceed the rate bound by the Global Sensitivity Setting:

1. Notify only of potential attack via Event Log (and/or SNMP Trap notice if configured)

OR

2. Notify and temporarily DENY information flow from the source client for a period of time bound by the Global Sensitivity Setting:

- ***LOW : between 0 and less than 30 seconds***
- ***MEDIUM: between 30 and less than 60 seconds***
- ***HIGH: between 60 and less than 90 seconds***

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- **AGGRESSIVE between 90 and 120 seconds**

AND THEN PERMIT information flow and re-evaluate the connection request rate coming from offending source client

OR

3. Notify and DENY all information flow from offending source client until system personnel re-enables that source client

].

FDP_IFF.1.4 (1) The TSF shall explicitly authorize an information flow based on the following rules:

[

IF

(Protocol Check)

1. Network traffic is IPv6 network traffic

OR

(Connection rate filtering disabled check)

2. Connection rate filtering has NOT been turned on for the specific inbound servicing switch port

OR

(Connection-Rate ACL Check)

3. ACL exists then:

If Source Client IP address is contained as an individually identified host

OR

If Source Client IP address is contained within an identified group of hosts

OR

If Source Client IP address is contained within an identified subnet

OR

If the UDP/TCP Criteria is contained within UDP/TCP Criteria of the Connection Rate ACL

AND

ACL entry is set to "ignore" (i.e. do not filter)

THEN

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

PERMIT information flow to Target Client(s)

].

FDP_IFF.1.5 (1) The TSF shall explicitly deny an information flow based on the following rules:

[

IF

Source Client has been blocked and not re-enabled

THEN

DENY information flow to target client(s)

].

6.1.3.3 FDP_IFC.1 (2) Subset information flow control (2)

Hierarchical to: No other components

Dependencies: FDP_IFF.1

FDP_IFC.1.1 (2) The TSF shall enforce the ***[MAC & Port Based Security Policy]*** on:

[

a) Subject:

Source Subjects: Source Client

Destination Subjects: Target Client(s)

b) Information:

Network traffic between Source subjects and Destination Subjects

c) Operation:

PERMIT information flow

DENY information flow

].

6.1.3.4 FDP_IFF.1 (2) Simple security attributes (2)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FDP_IFF.1.1 (2) The TSF shall enforce the **[MAC & Port Based Security Policy]** based on the types of subject and information security attributes:

[

a) Subject security attributes:

Source Subjects:

Source Port

MAC address of the Source Client

IP address of the Source Client

Destination Subject:

MAC address of the Target Client

b) Information security attributes:

- **Source Port (Inbound)**
- **Web and/or MAC Authentication enabled/disabled**
- **Web and/or MAC Authentication (with or without 802.1X) results**
- **Dynamic IP address Lockdown enabled/disabled**
 - **IP to MAC address binding list**
- **MAC Lockout enabled/disabled**
- **MAC Lockdown enabled/disabled**
- **Port Security enabled/disabled**
 - **Individual Authorized MAC address per port entry**
 - **Grouping of MAC addresses per port entry**
- **Eavesdrop-prevention enable/disable**

].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

[

Option 1: IF Web/MAC Authentication enabled on Source Port

Source Client MAC Address must be successfully authenticated via external service

OR

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Source Client Web Authentication must be successful authenticated via external service

THEN

PERMIT information flow and no further checks.

Else

Option 2: IF Dynamic IP Lockdown is enabled:

Source Client IP address is mapped to Source MAC address in address binding list for Source Port and VLAN pair

THEN

PERMIT information flow to Target Client(s); no further checks.

Else

Option 3: IF MAC Lockout or Lockdown is enabled:

1. MAC Lockout Check (system wide setting)

Source Client MAC Address is not equal to any MAC Lockout entries

AND

Target Client MAC Address is not equal to any MAC Lockout entries

AND

2. MAC Lockdown Check (port specific setting)

Target Client MAC Address must be contained in the MAC Lockdown List for the Port if enabled

AND

The Target Client must be on the specified port in the MAC and VLAN pair in the Lockdown list.

THEN

PERMIT information flow to Target Client(s); no further checks

Else

Option 4: IF Port Security is enabled:

1. Port Security Setting Check

If Port Security setting is enabled for the Source Port

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

AND

If Port is NOT part of a trunk group

AND

2. Source Check

If Source Client's MAC address is individually authorized to be on the Source Port (different than MAC Lockdown)

OR

If Source Client's MAC address is in contained the an authorized group of MAC addresses for the Source Port (different than MAC Lockdown)

OR

If Source Client's MAC address has been successfully authenticated via 802.1X

AND

3. Destination Check

If eavesdropping-prevention is enabled: Target Client(s) MAC address must be known to switch

THEN

PERMIT information flow to Target Client(s)

].

FDP_IFF.1.3 (2) The TSF shall enforce the ***[Manager configured responses if TOE DENIES information flow for:***

- **MAC Lockdown**
 - ***Notify of attempted use of port by another Source Client***
- **MAC Lockout**
 - ***Notify of attempted use of port by Locked out Source Client***
- **Port Security**
 - ***Notify only of potential attack via Event Log (and/or SNMP Trap notice if configured)***
 - ***Notify and block all traffic from offending source port until system personnel re-enables that client (host)***

].

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FDP_IFF.1.4 (2) The TSF shall explicitly authorize an information flow based on the following rules:

[

IF

The MAC address of Source Client does equal the Source Port's MAC lockdown configured Source Client MAC address

OR

The Port Security Setting is disabled for the Source Port

THEN

PERMIT information flow to Target Client(s)

].

FDP_IFF.1.5 (2) The TSF shall explicitly deny an information flow based on the following rules:

[

IF

MAC address of Source Client is contained in the MAC Lockout list

OR

The MAC address of Target Client is contained in the MAC Lockout list

OR

The MAC address of Target Client is contained in the MAC Lockdown list but is not on the specified port.

OR

Source Port has been disabled

OR

MAC address exceeds the number of MAC addresses the port has been configured to learn (retain).

THEN

DENY information flow to Target Client(s)

].

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

6.1.3.5 FDP_IFC.1 (3) Subset information flow control (3)

Hierarchical to: No other components

Dependencies: FDP_IFF.1

FDP_IFC.1.1 (3) The TSF shall enforce the **[Protocol Rate Limiting Security Policy]** on:

[

a) Subject:

Source Subjects: Source Client

Destination Subjects: Target Client(s)

b) Information:

Network traffic between Source subjects and Destination Subjects

c) Operation:

PERMIT information flow

DROP information flow

].

6.1.3.6 FDP_IFF.1 (3) Simple security attributes (3)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 (3) The TSF shall enforce the **[Protocol Rate Limiting Security Policy]** based on the types of subject and information security attributes:

[

a) Subject security attributes:

Source Subjects: Presumed IP address of the Source Client

Destination Subject: Presumed IP address of the Target Client(s)

b) Information security attributes:

- **Source port (inbound)**
- **Target port (outbound)**
- **Protocol (all or ICMP) of network traffic**
- **Bandwidth usage of traffic**

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- **Broadcast Rate Limit**
- **Multicast Rate Limit**
- **ICMP Limit setting**
 - **Inbound**
 - **Per port Setting (percentage)**
- **Rate Limit setting for all other traffic**
 - **Inbound**
 - **Port Setting (percentage or bits per second)**
 - **Outbound**

].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

[

IF rate-limit all is enabled:

1. Overall bandwidth usage for inbound network traffic on Source port is less than or equal to the Rate Limiting Inbound Port setting (defined as a percentage of overall bandwidth or in bits per second).

AND/OR

2. Overall bandwidth usage for outbound network traffic on Target port (s) is less than or equal to the Rate Limiting outbound Port setting (defined as a percentage of overall bandwidth or in bits per second)

THEN

PERMIT information flow to Target Client(s)

OR

(ICMP Inbound Check)

IF ICMP rate limiting is enabled:

1. Protocol on Source Port is ICMP

AND

2. ICMP bandwidth usage is less than or equal to the ICMP Limiting Inbound Port Setting (defined as a percentage of overall bandwidth)

THEN

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

PERMIT information flow to Target Client(s)

OR

(Broadcast Throttling Check)

IF Broadcast rate limiting is enabled:

1. The Target MAC address is Broadcast

AND

2. The rate is less than or equal to the Broadcast Rate Limit Threshold

THEN

PERMIT information flow to Target Client(s)

OR

(Broadcast Throttling Check)

IF Multicast rate limiting is enabled:

1. The Target MAC address is Multicast

AND

2. The rate is less than or equal to the Multicast Rate Limit Threshold

THEN

PERMIT information flow to Target Client(s)

].

FDP_IFF.1.3 (3) The TSF shall enforce the

[

DROPPING of any network traffic (inbound or outbound) that exceeds the Rate Limits (all, ICMP, Broadcast, Multicast) set

].

FDP_IFF.1.4 (3) The TSF shall explicitly authorize an information flow based on the following rules:

[

IF

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

rate limiting has NOT been turned on for the specific inbound servicing switch port

THEN

PERMIT information flow between source and target clients

].

FDP_IFF.1.5 (3) The TSF shall explicitly deny an information flow based on the following rules:

[

No additional rules based on Rate Limiting apply

].

6.1.3.7 FDP_IFC.1 (4) Subset information flow control (4)

Hierarchical to: No other components

Dependencies: FDP_IFF.1

FDP_IFC.1.1 (4) The TSF shall enforce the ***[Port and Protocol Filtering Security Policy]*** on:

[

a) Subject:

Source Subjects: Source Client

Destination Subjects: Target Client(s)

b) Information:

Network traffic between Source subjects and Destination Subjects

c) Operation:

PERMIT information flow

DROP information flow

].

6.1.3.8 FDP_IFF.1 (4) Simple security attributes (4)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 (4) The TSF shall enforce the ***[Port and Protocol Filtering Security Policy]*** based on the types of subject and information security attributes:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

[

a) *Subject security attributes:*

Source Subjects: Presumed IP address of the Source Client

Destination Subject: Presumed IP address of the Target Client(s)

b) *Information security attributes:*

- *Source port (inbound)*
- *Target port (outbound)*
- *Protocol of network traffic*
- *Port filtering enabled/disabled*
 - *(Setting forward, drop)*
- *Protocol filtering enabled/disabled*
 - *(Setting forward, drop)*

].

FDP_IFF.1.2 (4) The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

[

IF Port and Protocol Filtering is enabled

AND

1. IF Source Port's filter setting = "forward": THEN inbound network traffic on Source Port is PERMITTED only to the Target Port(s) identified in policy

OR

2. IF Protocol filter setting lists the permitted target ports: THEN inbound network traffic on Source Port is PERMITTED only to the Target Port(s) identified in policy

OR

3. IF Multicast filter setting="forward": THEN inbound network traffic on Source Port is PERMITTED only to the Target Port(s) identified in policy

].

Application Note: For DHCP requests: Restriction is based on a list of trusted Ports on which request could arrive.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FDP_IFF.1.3 (4) The TSF shall enforce the *[following:*

1. IF Source Port's filter setting = "drop": THEN inbound network traffic on Source Port is DROPPED.

OR

2. IF Source Port's Protocol filter setting ="drop": THEN inbound network traffic on Source Port is DROPPED.

OR

3. IF Source Port's Multicast filter setting="drop": THEN inbound network traffic on Source Port is DROPPED.

].

FDP_IFF.1.4 (4) The TSF shall explicitly authorize an information flow based on the following rules:

[

IF

Port and Protocol Filtering has NOT been turned on for the specific inbound servicing switch port

THEN

PERMIT information flow between Source and Target clients

].

FDP_IFF.1.5 (4) The TSF shall explicitly deny an information flow based on the following rules:

[

No additional rules based on Port and Protocol Filtering apply

].

6.1.3.9 FDP_IFC.1 (5) Subset information flow control (5)

Hierarchical to: No other components

Dependencies: FDP_IFF.1

FDP_IFC.1.1 (5) The TSF shall enforce the **[IPv4 ACL Security Policy]** on:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

[

a) Subject:

Source Subjects: Source Client

Destination Subjects: Target Client(s)

b) Information:

IPv4 Network traffic between Source subjects and Destination Subjects

c) Operation:

PERMIT information flow

DENY information flow

].

6.1.3.10 FDP_IFF.1 (5) Simple security attributes (5)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 (5) The TSF shall enforce the **[IPv4 ACL Security Policy]** based on the types of subject and information security attributes:

[

a) Subject security attributes:

Source Subjects:

IP address of the Source Client

Network mask of the Source Client

Network traffic protocol

Destination Subject:

IP address of Target Client

Network mask of the Target Client

b) Information security attributes:

- **Source Port (Inbound)**
- **Static ACL assigned port**
 - **Access Control Entry (ACE)**
 - **Standard**

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- **Source Address (SA) or “any”**
 - **SA can be a subnet, specific address, or group of addresses)**
- **Assigned Action: PERMIT or DENY**
- **Extended**
 - **Source Address (SA) or “any”**
 - **SA can be a subnet, specific address, or group of addresses)**
 - **Destination Address (DA) or “any”**
 - **Assigned Protocol for entry**
 - **Assigned Action: PERMIT or DENY**
- **VACL assigned to VLAN**
 - **Access Control Entry (ACE)**
 - **Source Address (SA) or “any”**
 - **SA can be a subnet, specific address, or group of addresses)**
 - **Assigned Protocol for entry**
 - **Destination Address (DA) or “any”**
 - **Assigned Action: PERMIT or DENY**
- **RACL assigned for routed traffic on VLAN**
 - **Access Control Entry (ACE)**
 - **Source Address (SA) or “any”**
 - **SA can be a subnet, specific address, or group of addresses)**
 - **Assigned Protocol for entry**
 - **Assigned Direction (IN or OUT)**
 - **Destination Address (DA) or “any”**
 - **Assigned Action: PERMIT or DENY**

].

FDP_IFF.1.2 (5) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

[

Option1: Static Standard ACL assigned to Source Port on switch

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

IF the Source Client IP Address matches an ACE entry's SA

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further option 1 checks.

Option 2: Static Extended ACL assigned to Source Port on switch

IF the Source Client IP Address matches an ACE entry's SA

AND

The Target Client IP Address equals "any"

OR

The Target Client IP Address matches the DA

AND

Traffic Protocol matches (or is contained within) the Assigned Protocol for entry

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

ELSE

IF the ACE entry's SA equals "any"

AND

The Target Client IP Address matches the DA

OR

The Target Client IP Address equals "any"

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

Option 3: VACL assigned to VLAN (a group of ports assigned to VLAN) on switch

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

IF the Source Client IP Address is within VLAN assignment

AND

Target Client IP Address is within same VLAN assignment

AND

Traffic Protocol matches the Assigned Protocol for entry

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

Option 4: RACL assigned to VLAN

IF Assigned Direction is "IN"

IF the Source Client IP Address is within VLAN assignment

AND

Traffic Protocol matches the Assigned Protocol for entry

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

IF Assigned Direction is "OUT"

IF the Target Client IP Address is within VLAN assignment

AND

Traffic Protocol matches the Assigned Protocol for entry

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

IF RACL has both Assigned Direction "IN" and "OUT"

IF the Source Client IP Address is within VLAN assignment

AND

If the Target Client IP Address is within VLAN assignment

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

AND

Traffic Protocol matches the Assigned Protocol for entry

AND

The Assigned Action is equal to PERMIT

THEN

PERMIT information flow and no further checks.

].

FDP_IFF.1.3 (5) The TSF shall enforce the **[Implicit Denial of traffic where the Source IP address does not match any of the ACE SA entries within the switch's source port/VLAN ACL.]**.

FDP_IFF.1.4 (5) The TSF shall explicitly authorize an information flow based on the following rules:

[

There is no ACL assigned to the Switch's Source Port/VLAN.

OR

The Switch's Source Port/VLAN has an assigned ACL with an ACE entry of "permit any" AND the Source Client IP address does not match any other ACE SA entry

OR

The Switch's Source Port/VLAN has an assigned ACL with an ACE entry of "permit IP any" AND the Source Client IP address does not match any other ACE SA entry

].

FDP_IFF.1.5 (5) The TSF shall explicitly deny an information flow based on the following rules:

[

The Switch's Source Port/VLAN has an assigned ACL with an the Source Client IP Address does not match any ACE entry

OR

The Switch's Source Port/VLAN has an assigned ACL with an ACE entry of "deny any" AND the Source Client IP address does not match any other ACE SA entry

OR

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

The Switch's Source Port/VLAN has an assigned ACL with an ACE entry of "deny IP any" AND the Source Client IP address does not match any other ACE SA entry

].

6.1.4 Class FIA: Identification and Authentication

6.1.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow ***[the execution of the Front-Panel Buttons' (Reset and Clear) Programmed Functions]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The TOE must be configured to require passwords for the 2 users (Manager and Operator) for minimal identification. If TOE is left in default mode, all functions would be available without authentication of user. Full individual user identification and authentication can only be achieved if TOE is configured so that I&A is handled via an external authentication server (RADIUS, TACACS+) or certificates see IA-4 for detailed information.

6.1.4.2 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide ***[Native Password Authentication]*** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

[

Following rules:

- ***Use Native Password Mechanism when enabled (default) AND no external authentication server is configured***

Else

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- **Invoke authentication request to the optionally configured external authentication mechanism**
- **Use Native Password mechanism when TSF fails to communicate with configured external authentication mechanism**

].

Application Note: The external authentication servers are NOT part of the TOE. The TOE only claims compatibility with RADIUS and TACACS+ servers).

6.1.4.3 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only **[asterisks for passwords]** to the user while the authentication is in progress.

6.1.4.4 FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow **[the execution of the Front-Panel Buttons' (Reset and Clear) Programmed Functions]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[Connection-Rate Based Security Policy, MAC & Port Based Security Policy, Protocol Rate Limiting Security Policy, Port and Protocol Filtering Security Policy]** to restrict the ability to **[change_default, modify, delete]** the security attributes **[security attributes listed in FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_IFF.1 (3)]** to **[Manager]**.

6.1.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[Connection-Rate Based Security Policy, MAC & Port Based Security Policy, Protocol Rate Limiting Security Policy, Port and Protocol Filtering Security Policy]** to provide **[permissive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[Manager]** to specify alternative initial values to override the default values when an object or information is created.

6.1.5.3 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to **[operations as specified in column 3 of Table 6-5]** the **[TSF data as specified in column 4 of Table 6-5]** to **[user security role as specified in column 2 of Table 6-5]**.

Table 6-5: Management of TSF data

Interface	User Security Role	Operations	TSF data
-----------	--------------------	------------	----------

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Interface	User Security Role	Operations	TSF data
CLI	Operator/Manager	Show <command>	Status and Counters <ul style="list-style-type: none"> • General System Information • Switch Management Address Information • Port Status • Port Counters • Address Table • Port Address Table • Front Panel Security Settings • Event logs
	Operator/Manager	Setup	Switch Configuration <ul style="list-style-type: none"> • System Information • Port/Trunk Settings • Network Monitoring Port • IP Configuration • SNMP Community Names • IP authorized Managers • VLAN Menu
	Operator/Manager	Ping <argument>	Connectivity test
	Operator/Manager	Link-test <argument>	Connectivity test
	Operator/Manager	Traceroute <argument>	Connectivity test
	Operator/Manager	Enable	Move from operator level to manager level (supply password)
	Operator/Manager	Menu	Switch to Menu Interface
	Operator/Manager	Logout	Exit from the CLI interface and terminate console session
	Operator/Manager	Exit	Terminate current session (same as logout)
	Manager	Set/Modify	Console Passwords
	Manager	Set/Modify	Set Usernames (pseudo names for Operator and Manager)
	Manager	Set/Modify	Inactivity Timeout
	Manager	Disable or re-enable	the password-clearing function of the Clear button.
	Manager	Configure	the Clear button to reboot the switch after clearing any local usernames and passwords
	Manager	Modify the operation of the Reset + Clear button combination	so that the switch reboots, but does not restore the switch's factory default settings.
	Manager	Disable or re-enable	password recovery.
	Manager	Config	Switch to Global Configuration
	Global Configuration	<Port or VLAN>	Change to Context Configuration

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Interface	User Security Role	Operations	TSF data	
Menu Interface	Operator/Manager	Show	Status and Counters • General System Information • Switch Management Address Information • Port Status • Port Counters • Address Table • Port Address Table	
	Operator/Manager	Show	Switch Configuration • System Information • Port/Trunk Settings • Network Monitoring Port • IP Configuration • SNMP Community Names • IP authorized Managers • VLAN Menu	
	Manager	Modify	Switch Configuration • System Information • Port/Trunk Settings • Network Monitoring Port • IP Configuration • SNMP Community Names • IP authorized Managers • VLAN Menu	
	Manager	Set/Modify	Console Passwords	
	Manager	Set/Modify	Inactivity Timeout	
	Operator/Manager	View	Event Log	
	Operator/Manager	Switch to CLI	Command Line (CLI)	
	Manager	Execute	Reboot Switch	
	Manager	Execute	Download OS (Download Switch Software)	
	Manager	Execute	Run Setup for quickly configuring basic switch parameters	
	Operator/Manager	Execute	Logout	
	Web Browser Interface	Operator	Read	Identity Tab
		Operator	Read	Status Tab
Operator		Read	Configuration Tab	
Operator		Read	Diagnostics Tab	
Operator		Read	Support Tab	
Manager		Read/Write	Identity Tab	
Manager		Read/Write	Status Tab	
Manager		Read/Write	Configuration Tab	
Manager		Read/Write	Security Tab	
Manager		Read/Write	Diagnostics Tab	
Manager		Read/Write	Support Tab	
Manager		Set/Modify	Console Passwords	

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Interface	User Security Role	Operations	TSF data
	Manager	Set/Modify	Set Usernames (pseudo names for Operator and Manager)
Physical Front Panel	N/A	clearing (removing) local password protection	The password and username (if it exists) associated with manager and operator levels used for authentication
	N/A	rebooting the switch	N/A
	N/A	restoring the switch to the factory default configuration (and erasing any non-default configuration settings)	Configuration data

6.1.5.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

[

- **operations as specified in column 3 of Table 6-5**
- **remote management (read/write) of the following MIB objects via optional external NMS station using SNMPv3**
- **number of primary and secondary login and enable attempts**
- **TACACS+ server configuration and status**
- **RADIUS server configuration**
- **selected 802.1X settings**
- **key management subsystem chain configuration**
- **key management subsystem key configuration**
- **OSPF interface authentication configuration**
- **local switch operator and manager usernames and passwords**

].

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

6.1.5.5 *FMT_SMR.1 Security roles*

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

- *Operator*
- *Manager*
- *Global Configuration (CLI only)*
- *Context Configuration (CLI only)*

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5.6 *FMT_SMR.3 Assuming roles*

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: **[For CLI users:**

- *Manager from Operator (enable),*
- *Global Configuration from Manager (config)*
- *Context Configuration from Global Configuration (<selected context>)*

].

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 *FPT_ITC_EXP.1 Explicit: Partial Inter-TSF confidentiality during transmission*

Hierarchical to: No other components

Dependencies: No dependencies

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

FPT_ITC_EXP.1.1 The TSF shall protect all TSF data transmitted from the TSF to the external **[authentication servers (RADIUS and TACACS+) and remote user management terminals]** from unauthorized disclosure during transmission.

6.1.6.2 FPT_TST_EXP.1 Explicit: TSF Self Testing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests **[during initial start-up and [reboot]]** to demonstrate the correct operation of the **[TSF]**.

FPT_TST_EXP.1.2 Upon detection of a test failure the TSF

[

can (depending on the error);

- **not complete boot,**
 - **light or flash fault LEDs,**
 - **generate a log entry,**
- **continue booting**
 - **disable a port from being used, or**
 - **disable a feature on the port (i.e. PoE)**
 - **generate a log entry**
 - **switchover of management model (Redundancy) [8200zl only]**

].

6.1.7 Class FTA: TOE access

6.1.7.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components

Dependencies: No dependencies

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

6.1.7.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[Manager assigned amount of time within the selection of < 0 | 1 | 5 | 10 | 15 | 20 | 30 | 60 | 120 > minutes (default 0 or off)]**.

6.2 Security Assurance Requirements for the TOE

This Section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL 2 augmented with ALC_FLR.1. None of the assurance components is refined. Table 6-6 summarizes the components.

Table 6-6: EAL2+ Assurance Components

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Architectural Design with Domain Separation and non-bypassability
	ADV_FSP.2	Security enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability Analysis

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-7 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

are denoted by an (H) following the dependency reference, explicitly stated SFRs are denoted by an (EXP) following the reference, and Operational Environment are denoted by an OE.

Table 6-7: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	Environment *
2	FAU_SAR.1	Audit Review	FAU_GEN.1	1
3	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
4	FCS_CKM.1	Cryptographic key generation	FCS_CKM.2 or FCS_COP.1	6
			FCS_CKM.4	5
5	FCS_CKM.4	Cryptographic key destruction	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	4
6	FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	4
			FCS_CKM.4	5
7	FDP_IFC.1 (1)	Subset information flow control (1)	FDP_IFF.1	8
8	FDP_IFF.1 (1)	Simple security attributes (1)	FDP_IFC.1	7
			FMT_MSA.3	22
9	FDP_IFC.1 (2)	Subset information flow control (2)	FDP_IFF.1	10
10	FDP_IFF.1 (2)	Simple security attributes (2)	FDP_IFC.1	9
			FMT_MSA.3	22
11	FDP_IFC.1 (3)	Subset information flow control (3)	FDP_IFF.1	12
12	FDP_IFF.1 (3)	Simple security attributes (3)	FDP_IFC.1	11
			FMT_MSA.3	22
13	FDP_IFC.1 (4)	Subset information flow control (4)	FDP_IFF.1	14
14	FDP_IFF.1 (4)	Simple security attributes (4)	FDP_IFC.1	13
			FMT_MSA.3	22
15	FDP_IFC.1 (5)	Subset information flow control (4)	FDP_IFF.1	16
16	FDP_IFF.1 (5)	Simple security attributes (4)	FDP_IFC.1	15
			FMT_MSA.3	22
17	FIA_UAU.1	Timing of authentication	FIA_UID.1	20
18	FIA_UAU.5	Multiple authentication mechanisms	None	N/A
19	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	17
20	FIA_UID.1	Timing of identification	None	N/A
21	FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1	7, 9, 11, 13, 15
			FMT_SMR.1	25
			FMT_SMF.1	24
22	FMT_MSA.3	Static attribute initialisation	FMT_MSA.1	21
			FMT_SMR.1	25
23	FMT_MTD.1	Management of TSF data	FMT_SMR.1	25
			FMT_SMF.1	24
24	FMT_SMF.1	Specification of Management Functions	None	N/A

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	SFR ID	SFR Title	Dependencies	Item Reference
25	FMT_SMR.1	Security roles	FIA_UID.1	20
26	FMT_SMR.3	Assuming roles	FMT_SMR.1	25
27	FPT_ITC_EXP.1	Explicit: Partial Inter-TSF confidentiality during transmission	None	N/A
28	FPT_TST_EXP.1	Explicit: TSF Self Testing	None	N/A
29	FTA_TAB.1	Default TOE access banners	None	N/A
30	FTA_SSL.3	TSF-initiated termination	None	N/A

** Note: Reliable timestamps are provided by the hardware and OS of the platforms that host the TOE components. See OE.Time as defined in Table 4-2: Security Objectives for the Operational Environment.*

6.3.2 Functional Requirements

Table 6-8 traces each SFR back to the security objectives for the TOE.

Table 6-8: Mapping of TOE SFRs to TOE Security Objectives

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1	O.AuditGeneration
2	FAU_SAR.1	O.AuditReview
3	FAU_STG.1	O.AuditProtect
4	FCS_CKM.1	O.CryptoSupport
5	FCS_CKM.4	O.CryptoSupport
6	FCS_COP.1	O.CryptoSupport
7	FDP_IFC (1)	O.RateBased
8	FDP_IFF (1)	O.RateBased
9	FDP_IFC (2)	O.UndesiredAccess
10	FDP_IFF (2)	O.UndesiredAccess
11	FDP_IFC (3)	O.ProtocolFiltering
12	FDP_IFF (3)	O.ProtocolFiltering
13	FDP_IFC (4)	O.ProtocolFiltering O.UndesiredAccess
14	FDP_IFF (4)	O.ProtocolFiltering O.UndesiredAccess
15	FDP_IFC (5)	O.UndesiredAccess
16	FDP_IFF (5)	O.UndesiredAccess
17	FIA_UAU.1	O.RobustTOEAccess
18	FIA_UAU.5	O.RobustTOEAccess
19	FIA_UAU.7	O.ProtectAuth
20	FIA_UID.1	O.RobustTOEAccess
21	FMT_MSA.1	O.RateBased, O.UndesiredAccess, O.ProtocolFiltering
22	FMT_MSA.3	O.RateBased, O.UndesiredAccess, O.ProtocolFiltering
23	FMT_MTD.1	O.Access
24	FMT_SMF.1	O.Manage
25	FMT_SMR.1	O.Access

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	SFR ID	TOE Security Objective
26	FMT_SMR.3	O.AssumingRoles
27	FPT_ITC_EXP.1	O.TransProtect, O.ProtectComm
28	FPT_TST_EXP.1	O.SelfTest
29	FTA_TAB.1	O.Banner
	FTA_SSL.3	O.InactivityTermination

Table 6-9 demonstrates that the SFRs meet all security objectives for the TOE. Rationale for each objective is included in the table.

Table 6-9: All TOE Objectives Met by Security Functional Requirements

Item	Objective ID	Objective Description	SFR ID	Rationale
1	O.Access	The TOE will allow access to the protected management functions and TSF data only to authorized users with the appropriate security roles via the TOE management interfaces.	FMT_MTD.1	FMT_MTD.1 specifies the administrative functions and the TSF data on which they operate as they are available to each of the defined administrative (security) roles for each of the administrative interfaces of the TOE.
			FMT_SMR.1	FMT_SMR.1 requires that the TSF maintain multiple administrative roles. The TSF is able to associate a human user with one or more administrative roles and these roles are used to restrict access (access control) to the administrative functions and TSF data.
2	O.AssumingRoles	The TOE will require that an explicit request along with a password must be given to assume (change to a) the Manager role from an Operator Role.	FMT_SMR.3	FMT_SMR.3 defines the requirement that in order for a user to change (assume) a different roll that it must be explicitly requested.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Objective ID	Objective Description	SFR ID	Rationale
3	O.AuditGeneration	The TOE will provide the capability to create records of security-relevant events and associate these events with the process which caused the event.	FAU_GEN.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event.
4	O.AuditProtect	The TOE will protect its own audit trail from unauthorized modification and deletion.	FAU_STG.1	FAU_STG.1 defines the requirement that the TOE protect its own audit trail from unauthorized deletion and modification.
5	O.AuditReview	The TOE will provide the capability for review of the audit information to authorized users via the TOE's protected management interfaces.	FAU_SAR.1	FAU_SAR.1 defines the requirement of the TOE to provide an audit review capability via the protected management interfaces (those requiring a successful I&A).
6	O.Banner	The TOE will display an access banner prior/during Login process. This banner will be customizable by the administrators.	FTA_TAB.1	FTA_TAB.1 defines that an access banner be displayed before establishing a user session. The TSF is capable of displaying a customizable banner as part of the login process but prior to establishing a user session.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Objective ID	Objective Description	SFR ID	Rationale
7	O.CryptoSupport	The TOE will provide cryptographic functions for protecting TSF data during transmission to another IT trusted product.	FCS_CKM.1	FCS_CKM.1 defines the key generation parameters for the cryptographic operations used for secure communications or encryption of TSF data.
			FCS_CKM.4	FCS_CKM.4 defines the method of destroying the keys used in the cryptographic operations used for secure communications or encryption of TSF data.
			FCS_COP.1	FCS_COP.1 defines the parameters of the cryptographic operations used by the TOE for secure communications or encryption of TSF data.
8	O.InactivityTermination	The TOE will terminate a session due to an administratively defined period of inactivity.	FTA_SSL.3	FTA_SSL.3 defines the requirement that the TOE terminates an interactive session after a specified timeframe. The TOE implements a forced logout/termination of a user session that has been inactive for a period of time.
9	O.Manage	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.	FMT_SMF.1	FMT_SMF.1 requires the TSF be capable of performing the specified security management functions.
10	O.ProtectAuth	The TOE will provide protected authentication feedback.	FIA_UAU.7	FIA_UAU.7 specifies that the user's password will be masked on input.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Objective ID	Objective Description	SFR ID	Rationale
11	O.RobustTOEAccess	The TOE will provide a native I&A mechanism and the functionality to invoke optional external I&A mechanisms to control the user's logical access to the protected interfaces of the TOE.	FIA_UAU.1	FIA_UAU.1 specifies that there are some management functions that can be implemented prior to being identified or authenticated. The TOE protects management interfaces other than the Front Panel Switches that must be protected by the environment.
			FIA_UAU.5	FIA_UAU.5 specifies that the TOE provides some I&A features natively and that it also provides functionality to invoke external entities to provide I&A decisions.
			FIA_UID.1	FIA_UID.1 specifies that there are some management functions that can be implemented prior to being identified or authenticated. The TOE protects management interfaces other than the Front Panel Switches that must be protected by the environment.
12	O.SelfTest	The TOE will automatically run a series of self tests during boot to ensure the proper operation of the hardware and software modules of the TOE.	FPT_TST_EXP.1	FPT_TST_EXP.1 defines the requirement to provide a mechanism that will verify the correct operation of the hardware and software modules during initialization. The TOE may not attain operational state if the initialization tests do not complete successfully. Initialization or execution follows a predefined set of procedures if a failure occurs.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Objective ID	Objective Description	SFR ID	Rationale
13	O.TransProtect	The TOE must protect all TSF data from unauthorized disclosure during transmission to the external authentication server by ensuring that a secure channel is used.	FPT_ITC_EXP.1	FPT_ITC_EXP.1 defines that the TSF will protect, in conjunction with the operational environment, TSF data that is transmitted to the external I&A servers.
14	O.UndesiredAccess	The TOE must control unauthorized information flow between internal and external networks based on security policies.	FDP_IFC (2) FDP_IFF (2) FDP_IFC (4) FDP_IFF (4) FDP_IFC (5) FDP_IFF (5)	FDP_IFC.1 (2,4 & 5), FDP_IFF.1 (2,4 & 5) defines the policies to control flow between clients based on controlling the source and destination ports of the switch, Source and Target IP addresses, Flow within VLAN and between VLANs.
			FMT_MSA.1 FMT_MSA.3	FMT_MSA.1 and FMT_MSA.3 defines that the attributes for the all the IFF Security Policies are permissive and restricts the modification of the attributes to the role of Manager.
15	O.RateBased	The TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DoS and DDoS attacks, and authorized users who may overuse resources.	FDP_IFC (1) FDP_IFF (1)	FDP_IFC.1 (1) and FDP_IFF.1 (1) defines the policy to control flow between clients based on controlling the rate of connection requests coming from a single source on a port. If too many requests the TOE can automatically respond by temporarily or permanently blocking the source client.
			FMT_MSA.1 FMT_MSA.3	FMT_MSA.1 and FMT_MSA.3 defines that the attributes for the all the IFF Security Policies are permissive and restricts the modification of the attributes to the role of Manager.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Item	Objective ID	Objective Description	SFR ID	Rationale
16	O.ProtocolFiltering	The TOE must be able to perform protocol-based filtering, which includes forwarding, dropping, automatic throttling of ICMP, or automatic throttling of all protocol traffic.	FDP_IFC (3) FDP_IFF (3) FDP_IFC (4) FDP_IFF (4)	FDP_IFC.1 (3 & 4) and FDP_IFF.1 (3 & 4) defines the policy to control flow between clients based on controlling the forwarding, dropping, and the rate or amount of bandwidth that any protocol may use (inbound or outbound). ICMP protocol rate filtering (inbound only) is a separate entity within the policy.
			FMT_MSA.1 FMT_MSA.3	FMT_MSA.1 and FMT_MSA.3 defines that the attributes for the all the IFF Security Policies are permissive and restricts the modification of the attributes to the role of Manager.
17	O.ProtectComm	The TOE must protect all TSF data from unauthorized disclosure during transmission to the remote user management terminal by ensuring that a secure channel is used.	FPT_ITC_EXP.1	FPT_ITC_EXP.1 defines that the TSF will protect TSF data that is transmitted to another the remote user management terminal.

6.3.3 Assurance Rationale

Evaluation Assurance Level EAL2 augmented with ALC_FLR was chosen to provide a moderate level of assurance due to the requirements of DoD customer.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

7 TOE Summary Specification

7.1 IT Security Functions

Section 7.1 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions From Logical Scope	Sub-Functions	SFRs
Audit Functionality	SA-1 Audit Generation	FAU_GEN.1 FAU_STG.1
	SA-2 Audit Review	FAU_SAR.1
	IA-1 Password Masking	FIA_UAU.7
User I&A Functions	IA-2 User Identification	FIA_UID.1
	IA-3 User Authentication	FIA_UAU.1 FIA_UAU.5
	Information Flow Control	IFC-1 Connection-Rate Based Security Policy
FDP_IFF.1 (1)		
FMT_MSA.1		
FMT_MSA.3		
IFC-2 MAC & Port Based Security Policy		FDP_IFC.1 (2)
		FDP_IFF.1 (2)
		FMT_MSA.1
		FMT_MSA.3
IFC-3 Protocol Rate Limiting Security Policy		FDP_IFC.1 (3)
		FDP_IFF.1 (3)
		FMT_MSA.1
		FMT_MSA.3
IFC-4 Port and Protocol Filtering Security Policy		FDP_IFC.1 (4)
		FDP_IFF.1 (4)
		FMT_MSA.1
	FMT_MSA.3	
IFC-5 ACL Filtering Security Policy	FDP_IFC.1 (5)	
	FDP_IFF.1 (5)	
	FMT_MSA.1	
	FMT_MSA.3	
Security Management with Access Control	SM-1 Management Functions	FMT_SMF.1
	SM-2 Management Security Roles	FMT_SMR.1 FMT_SMR.3
	SM-3	FMT_MTD.1

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Security Functions From Logical Scope	Sub-Functions	SFRs
	Management Access Control	FMT_SMR.1
TOE Access	TA-1 Login Banner	FTA_TAB.1
	TA-2 Inactivity Termination	FTA_SSL.3
Protection of TSF	TP-1 Cryptographic Support	FCS_CKM.1
		FCS_CKM.4
		FCS_COP.1
	TP-2 Self Testing	FPT_ITC_EXP.1

7.1.1 Audit Functionality

7.1.1.1 SA-1: Audit Generation

(FAU_GEN.1, FAU_STG.1)

The Event Log records operating events in single- or double-line entries and serves as a tool to isolate and troubleshoot problems. The maximum number of entries supported in the Event Log is 2000 entries. Entries are listed in chronological order, from the oldest to the most recent. Once the log has received 2000 entries, it discards the oldest message each time a new message is received.

The audit trail is stored on the switch and is accessible via the protected management functional interfaces (see SM-2).

The TOE can protect the Event Log from unauthorized deletion or modification. The Event Log will be erased (not protected) if power to the switch is interrupted or if the boot system command is used. The contents of the Event Log will not be erased if the following actions are taken:

- Reboot the switch by choosing the Reboot Switch option from the menu interface.
- Enter the reload command from the CLI.

The TOE does support the exporting of audit records to a central Syslog server. The Syslog server is external and not part of the TOE. Certain audit events can also be configured to trigger an SNMP trap and sent to a System management server. The System Management server is external and not part of the TOE.

Event Log Entries

Each Event Log entry is composed of five or six fields, depending on whether numbering is turned on or not:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Severity	Date	Time	Event number	System Module	Event Message
I	08/05/06	10:52:32	00063	ports:	port A1 enabled

Figure 4: Format of an Event Log Entry

Severity is one of the following codes (from highest to lowest severity):

- **M** (major) indicates that a fatal switch error has occurred.
- **E** (error) indicates that an error condition occurred on the switch.
- **W** (warning) indicates that a switch service has behaved unexpectedly.
- **I** (information) provides information on normal switch operation.
- **D** (debug) is reserved for HP Networking internal diagnostic information.

Date is the date in the format mm/dd/yy when an entry is recorded in the log.

Time is the time in the format hh:mm:ss when an entry is recorded in the log.

Event Number is the number assigned to an event. Event numbering can be turned on and off with the [no] log-number command.

System Module is the internal module (such as “ports:” for port manager) that generated a log entry. If VLANs are configured, then a VLAN name also appears for an event that is specific to an individual VLAN

Event Message is a brief description of the operating event.

Operational Environment Support

SA-1: Audit Generation is supported by the Operational Environment through:

- Use of time server that uses either TimeP or SNTP time synchronization protocols. The switch does provide for a battery backup to continue to produce a timestamp in the case that the time synch server goes offline.
- Physical protection of the switch at a level commensurate that is consistent with the operating environment.
- Use of an optional Syslog server
- Use of an option System Management server to receive optional SNMP traps that mirror event logs that are stored in the local audit trail.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

7.1.1.2 SA-2: Audit Review

(FAU_SAR.1)

The TOE provides both Managers and Operators to view the Event Log via the Menu Interface and CLI.

Menu: Displaying and Navigating in the Event Log

To display the Event Log from the Main Menu, select Event Log.

```
ProCurve Switch 5406zl                               25-Oct-2007 18:02:52
-----CONSOLE - MANAGER MODE -----
M 10/25/07 16:30:02 sys: "Operator cold reboot from CONSOLE session."
I 10/25/07 17:42:51 00061 system: -----
I 10/25/07 17:42:51 00063 system: System went down: 10/25/07 16:30:02
I 10/25/07 17:42:51 00064 system: Operator cold reboot from CONSOLE session.
W 10/25/07 17:42:51 00374 chassis: WARNING: SSC is out of Date: Load 8.2 or newer
I 10/25/07 17:42:51 00068 chassis: Slot D Inserted
I 10/25/07 17:42:51 00068 chassis: Slot E Inserted
I 10/25/07 17:42:51 00068 chassis: Slot F Inserted
I 10/25/07 17:42:51 00690 udpf: DHCP relay agent feature enabled
I 10/25/07 17:42:51 00433 ssh: Ssh server enabled
I 10/25/07 17:42:52 00400 stack: Stack Protocol disabled
I 10/25/07 17:42:52 00128 tftp: Enable succeeded
I 10/25/07 17:42:52 00417 cdp: CDP enabled

---- Log events stored in memory 1-751. Log events on screen 690-704.

Actions->  Back      Next page  Prev page  End      Help

Return to previous screen.
Use up/down arrow to scroll one line, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 5: Example of an Event Log Display

The log *status line* below the recorded entries states the total number of events stored in the event log and which logged events are currently displayed. To scroll to other entries in the Event Log, either preceding or following the currently visible portion, press the keys indicated at the bottom of the display (**Back**, **Next page**, **Prev page**, or **End**) or the keys described below.

Key Action

[N] Advances the display by one page (next page).

[P] Rolls back the display by one page (previous page).

[v] Advances display by one event (down one line).

[^] Rolls back display by one event (up one line).

[E] Advances to the end of the log.

[H] Displays Help for the Event Log.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

CLI: Displaying the Event Log

To display messages recorded in the event log from the CLI, enter the **show logging** command. Keyword searches are also supported.

Syntax: show logging [-a, -r] [<search-text>]

By default, the show logging command displays the log messages recorded since the last reboot in chronological order.

-a displays all recorded log messages, including those before the last reboot.

-r displays all recorded log messages, with the most recent entries listed first.

<search-text> displays all Event Log entries that contain the specified text.

Use a <search-text> value with -a or -r to further filter show logging command output.

Examples:

To display all Event Log messages that have “system” in the message text or module name, enter the following command:

```
HP_switch# show logging -a system
```

To display all Event Log messages recorded since the last reboot that have the word, “system”, in the message text or module name, enter:

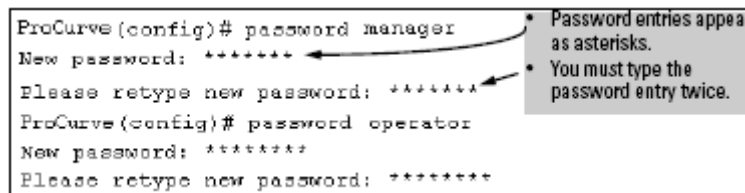
```
HP_switch# show logging system
```

7.1.2 User I&A Functions

7.1.2.1 IA-1: Password Masking

(FIA_UAU.7)

The TOE masks the entry of password using asterisks. Passwords are masked for all password logins and the setting/modification of the passwords. At no time are passwords displayed in the open. An example of this is shown in the figure below



```
ProCurve(config)# password manager
New password: *****
Please retype new password: *****
ProCurve(config)# password operator
New password: *****
Please retype new password: *****
```

• Password entries appear as asterisks.
• You must type the password entry twice.

Figure 6: Example of Masked Passwords during creation using CLI

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

7.1.2.2 IA-2: User Identification

(FIA_UID.1)

The TOE provides the customer with the ability to execute the Management functions that use the Front Panel Buttons without identification. It is expected that the TOE will be configured to ensure that both the Manager and Operator (or their associated usernames) have passwords assigned to restrict usage of Management functions that use the CLI, Menu Interface, and Web Browser until after identification and authentication have occurred. Manager and Operator would be considered the minimal acceptable identification. Further individual identification may be obtained by using one of the supported external authentication mechanisms described under User Authentication.

Front-Panel Button Functions

It used to be assumed that only system and network administrators would be able to get access to a network switch because switches were typically placed in secure locations under lock and key. For some customers this is no longer true. Others simply want the added assurance that even if someone did manage to get to the switch that data would still remain secure.

User-defined passwords can easily be deleted by pushing the **Clear** button on the front panel, if front-panel security on the switch does not get invoked. This function exists so that if customers forget the defined passwords they can still get back into the switch and reset the passwords. This does, however, leave the switch vulnerable when it is located in an area where non-authorized people have access to it. Someone who has physical access to the switch may be able to erase the passwords (and possibly configure new passwords) and take control of the switch.

The TOE provides the customers the ability to stop someone from removing passwords by disabling the **Clear** and/or **Reset** buttons on the front of the switch for increased security.

The System Support Module (SSM) of the switch includes the **System Reset** button and the **Clear** button.

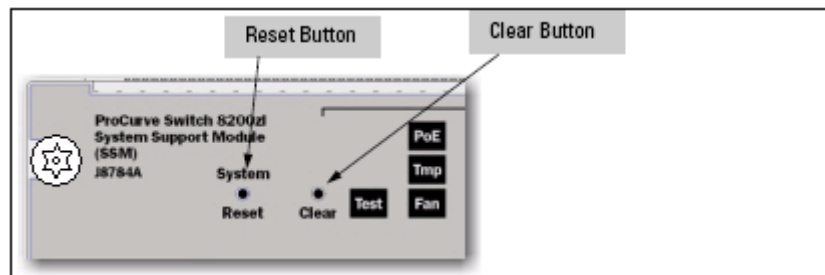


Figure 7: Front Panel Buttons

The following is what can be accomplished when the advanced security features are not used.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Table 7-2: Front Panel Button Actions

Reset	Clear	Steps	Results
	X	Press and hold for 1 second	Resets passwords configured on the switch
X		Press and hold for 1 second	Reboots the switch
X	X	1. Press and hold the Reset button 2. While holding the Reset button, press and hold the Clear button 3. Release the Reset button 4. When the Test LED to the right of the Clear button begins flashing, release the Clear button.	Restores switch to default settings and reboots (can take 20-25 seconds to reboot)

The TOE provides the ability to configure the buttons to have different results than above.

Using the front-panel-security command from the global configuration context in the CLI the Manager can:

- Disable or re-enable the password-clearing function of the **Clear** button. Disabling the **Clear** button means that pressing it does not remove local password protection from the switch. (This action affects the **Clear** button when used alone, but does not affect the operation of the **Reset + Clear** combination described for “Restoring the Factory Default Configuration”.)
- Configure the **Clear** button to reboot the switch after clearing any local usernames and passwords. This provides an immediate, visual means (plus an Event Log message) for verifying that any usernames and passwords in the switch have been cleared.
- Disable the password-clear function of the **Clear** button, so that pressing it has no effect on any local usernames and passwords. (Using **Reset + Clear** is not affected.)
- Modify the operation of the **Reset + Clear** combination so that the switch still reboots, but does not restore the switch’s factory default configuration settings. and/or doesn’t remove local usernames and passwords. (Use of the **Reset** button alone, to simply reboot the switch, is not affected.)
- Disable or re-enable Password Recovery. The password recovery feature is enabled by default and provides a method for regaining management access to the switch (without resetting the switch to its factory default configuration) in the event that the system administrator loses the local manager username (if configured) or password. Using Password Recovery requires:
 - **password-recovery** enabled (the default) on the switch prior to an attempt to recover from a lost username/password situation
 - Contacting the HP Networking Customer Care Center to acquire a one-time use password

*Note: Disabling **password-recovery** requires that **factory-reset** be enabled, and locks out the ability to recover a lost manager username (if configured) and password on the switch. In this event, there is no way to recover from a lost manager username/password situation without resetting the switch to its factory-default configuration. This can disrupt*

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

*network operation and make it necessary to temporarily disconnect the switch from the network to prevent unauthorized access and other problems while it is being reconfigured. Also, with **factory-reset** enabled, unauthorized users can use the **Reset + Clear** button combination to reset the switch to factory-default configuration and gain management access to the switch.*

- Change console ports inactivity timer to a value other than the default of 0 (which means no forced end of session even if cable is disconnected). See TA-2 below for details on implementation.

Operational Environment Support

IA-2: User Identification is supported by the Operational Environment through:

- Use of an optional authentication server
- Physical protection of switch at a level commensurate that is consistent with the operating environment.
- Support for the trusted communications implementation required to interface with optional authentication servers.

7.1.2.3 IA-3: User Authentication

(FIA_UAU.1, FIA_UAU.5)

The TOE Management functions that are allowed prior to authentication are the same as those defined in IA-2.

A Manager **must** configure the password associated with the two user roles via the CLI, Menu Interface, and/or Web Interface. After the Manager configures or modifies a password, the next subsequent start of a new console session, the user will be prompted to enter the new password. If the Manager used the CLI or web browser interface to also configure an optional username, the switch will prompt for the username, and then the password.

Note: There is only one password for all users acting as Managers (or Operators).

If individual username/password protection is desired/required the TOE must be configured to invoke an alternative operational environment authentication server (RADIUS or TACACS+).

The TOE enforces a case sensitive password of up to 16 characters. There is no minimum password length enforced by the TOE. Therefore, for CC compliance the organization must enforce a password policy of at least 8 characters and should have at least 3 of the following 1 upper, 1 lower, 1 numeric, and/or 1 special character. Passwords are saved in hashed (SHA-1) format.

The TOE supports the following character sets:

- A through Z (uppercase characters)
- a through z (lowercase characters)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

0 through 9 (numeric characters)

Special characters: ` ~ ! @ # \$ % ^ & * () - _ = + [] { } \ | ; : ' " , < > / ?

CLI: Setting Passwords and Usernames

To set the passwords and optional username (pseudo name for Manager and Operator roles) using CLI the Manager must use the **password** command.

Syntax: [no] password <manager | operator | all | port-access>
[username ASCII-STR] [<plaintext | sha1> ASCII-STR]

```
ProCurve(config)# password manager
New password: *****
Please retype new password: *****
ProCurve(config)# password operator
New password: *****
Please retype new password: *****
```

• Password entries appear as asterisks.
• You must type the password entry twice.

Figure 8: Example of Configuring Manager and Operator Passwords

Menu: Setting Passwords

As noted earlier in this section, usernames are optional. Configuring a username requires either the CLI or the web browser interface.

1. From the Main Menu select:

3. Console Passwords

```
----- CONSOLE - MANAGER MODE -----
Set Password Menu

1. Set Operator Password
2. Set Manager Password
3. Delete Password Protection
0. Return to Main Menu...

Prompts you to enter an Operator-level password.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 9: The Set Password Screen

2. To set a new password:

a. Select **Set Manager Password** or **Set Operator Password**. Enter new password prompt is displayed.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- b. Type a password of up to 16 ASCII characters with no spaces and press **Enter** (passwords are case-sensitive.).
- c. When prompted with **Enter new password again**, retype the new password and press [Enter].

Web: Setting Passwords and Usernames

In the web browser interface passwords and (optional) usernames can be entered.

To Configure Usernames and Passwords in the Web Browser Interface:

1. Click on the **Security** tab.

Click on **Device Passwords**

2. Do one of the following:

- To set username and password protection, enter the usernames and passwords in the appropriate fields.
- To remove username and password protection, leave the fields blank.

3. Implement the usernames and passwords by clicking on **Apply Changes**.

SNMP: Setting Passwords and Usernames

In Software Version K.15.09.04 (and KA.15.09.04) usernames and passwords for Manager and Operator access can also be configured using SNMP. With SNMP access to the hpSwitchAuth MIB enabled, a device with management access to the switch can view the configuration for the authentication features listed below (excluding usernames, passwords, and keys). Using SNMP sets, a management device can change the authentication configuration (including changes to usernames, passwords, and keys). Operator read/write access to the authentication MIB is always denied.

Manager-only SNMP read/write access to a subset of the authentication MIB objects for the following features is allowed:

- number of primary and secondary login and enable attempts
- TACACS+ server configuration and status
- RADIUS server configuration
- selected 802.1X settings
- key management subsystem chain configuration
- key management subsystem key configuration
- OSPF interface authentication configuration
- local switch operator and manager usernames and passwords

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

All usernames, passwords, and keys configured in the hpSwitchAuth MIB are not returned via SNMP, and the response to SNMP queries for such information is a null string. However, SNMP sets can be used to configure username, password, and key MIB objects.

To help prevent unauthorized access to the switch's authentication MIB, HP Networking recommends enhancing security according to the guidelines under "Switch Access Security" on page 1-3 of the *Access Security Guide* which is also outlined in SM-3: Management Access Control :SNMP Access below.

SNMP access to the switch's authentication configuration MIB can be disabled with the **snmp-server mib hpswitchauthmib excluded** command.

If it is required to leave SNMP access to the security MIB open (the default setting), then HP Networking recommends that the switch be configured with the SNMP version 3 management and access security feature, and disable the SNMP version 2c access.

External TACACS+ Authentication

The TOE can be configured to invoke an external authentication mechanism called a TACACS+ server to make access control decisions. The TACACS+ server is not part of the TOE, but the TOE contains logic to communicate specifically with such a server. The TOE can invoke the external authentication server for access requests from either the switch's serial (console) port or for SSH connection. If the switch fails to connect to a TACACS+ server for the necessary authentication service, it defaults to its own locally configured passwords for authentication control.

External RADIUS Authentication

The TOE can be configured to invoke an external authentication mechanism called a RADIUS server to make access control decisions. The RADIUS server is not part of the TOE, but the TOE contains logic to communicate specifically with such a server. The TOE can invoke the external authentication server for access requests from

- Serial port (Console)
- SSH
- SFTP/SCP
- SSL
- Port-Access (802.1X)

The switch does not support RADIUS security for SNMP

If the switch fails to connect to a RADIUS server(s) for the necessary authentication service, it defaults to its own locally configured passwords for authentication control.

Operational Environment Support

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

IA-3: User Identification and User Authentication is supported by the Operational Environment through:

- Physical protection of switch
- Network support
- Network Management Server (SNMPv3) [optional]
- 802.1X client application [optional]
- RADIUS Server [optional]
- TACACS+ Server [optional]

7.1.3 Information Flow Control

7.1.3.1 IFC-1 Connection-Rate Based Security Policy

(FDP_IFC.1 (1), FDP_IFF.1 (1), FMT_MSA.1, FMT_MSA.3)

Connection-Rate Based Security Policy is referred to by the vendor as “Virus Throttling”. Virus Throttling is implemented through connection-rate filtering. When connection-rate filtering is enabled on a port, the inbound routed traffic is monitored for a high rate of connection requests from any given host on the port. If a host appears to exhibit the worm-like behavior of attempting to establish a large number of outbound IP connections in a short period of time, the switch responds on the basis of how connection-rate filtering is configured.

Virus Throttle works by intercepting IP connection requests, that is, connections in which the source subnet and destination address are different. The Virus Throttle tracks the number of recently made connections. If a new, intercepted request is to a destination to which a connection was recently made, the request is processed as normal. If the request is to a destination that has not had a recent connection, the request is processed only if the number of recent connections is below a pre-set threshold. The threshold specifies how many connections are to be allowed over a set amount of time, thereby enforcing a connection rate limit. If the threshold is exceeded, because requests are coming in at an unusually high rate, it is taken as evidence of a virus. This causes the throttle to stop processing requests and, instead, to notify the system administrator.

This capability can be applied to most common Layer 4 through 7 session and application protocols, including TCP connections, UDP packets, SMTP, IMAP, Web Proxy, HTTP, SSL, and DNS—virtually any protocol where the normal traffic does not look like a virus spreading. For Virus Throttle to work, IP routing and multiple VLANs with member ports must first be configured.

Note: Some protocols, such as NetBIOS and WINS, and some applications such as network management scanners, notification services, and p2p file sharing are not appropriate for Virus Throttle. These protocols and applications initiate a broad burst of network traffic that could be misinterpreted by the Virus Throttle technology as a threat.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Syntax: filter connection-rate < port-list > < notify-only | throttle | block > no filter
connection-rate < port-list >

Response options

The response behavior of connection-rate filtering can be adjusted by using filtering options. When a worm-like behavior is detected, the connection-rate filter can respond to the threats on the port in the following ways:

- Notify only of potential attack: While the apparent attack continues, the switch generates an Event Log notice identifying the offending host source address (SA) and (if a trap receiver is configured on the switch) a similar SNMP trap notice.
- Notify and reduce spreading: In this case, the switch temporarily blocks inbound routed traffic from the offending host source address for a “penalty” period and generates an Event Log notice of this action and a similar SNMP trap notice if a trap receiver is configured on the switch. When the penalty period expires, the switch re-evaluates the routed traffic from the host and continues to block this traffic if the apparent attack continues. During the re-evaluation period, routed traffic from the host is allowed.
- Block spreading: This option blocks routing of the host’s traffic on the switch. When a block occurs, the switch generates an Event Log notice and a similar SNMP trap notice if a trap receiver is configured on the switch.

Note: System personnel must explicitly re-enable a host that has been previously blocked.

Global Sensitivity Setting

The ability of connection-rate filtering to detect relatively high instances of connection-rate attempts from a given source can be adjusted by changing the global sensitivity settings. The sensitivity can be set to low, medium, high, or aggressive as described here:

- Low: sets the connection-rate sensitivity to the lowest possible sensitivity, which allows a mean of 54 routed destinations in less than 0.1 seconds, and a corresponding penalty time for Throttle mode (if configured) of less than 30 seconds
- Medium: sets the connection-rate sensitivity to allow a mean of 37 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 30 and 60 seconds
- High: sets the connection-rate sensitivity to allow a mean of 22 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 60 and 90 seconds
- Aggressive: sets the connection-rate sensitivity to the highest possible level, which allows a mean of 15 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 90 and 120 seconds

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Connection-Rate ACL

Connection-rate ACLs are used to exclude legitimate high-rate inbound traffic from the connection-rate filtering policy. A connection-rate ACL, consisting of a series of access control entries, creates exceptions to these per-port policies by creating special rules for individual hosts, groups of hosts, or entire subnets. The ACL rules take precedence over other filtering rules (thus allowing for the exceptions).

7.1.3.2 IFC-2 Port Based Security Policy

(FDP_IFC.1 (2), FDP_IFF.1 (2), FMT_MSA.1, FMT_MSA.3)

Web - MAC Authentication

Web and MAC authentication are designed for employment on the “edge” of a network to provide port-based security measures for protecting private networks and a switch from unauthorized access. Because neither method requires clients to run special supplicant software (unlike 802.1X authentication), both Web and MAC authentication are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Only a web browser (for Web authentication) or a MAC address (for MAC authentication) is required.

Both Web and MAC authentication methods rely on a RADIUS server (which is outside the TOE) to authenticate network access. This simplifies access security management by allowing you to control access from a master database in a single server. (Up to three RADIUS servers can be used to provide backups in case access to the primary server fails.) It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN.

On a port configured for Web or MAC Authentication, the switch operates as a port-access authenticator using a RADIUS server and the CHAP protocol (Challenge Handshake Authentication Protocol, also known as “CHAP-RADIUS”). Inbound traffic is processed by the switch alone, until authentication occurs. Some traffic from the switch to an unauthorized client is supported (for example, broadcast or unknown destination packets) before authentication occurs.

The **Web Authentication (Web-Auth)** method uses a web page login to authenticate users for access to the network. When a client connects to the switch and opens a web browser, the switch automatically presents a login page.

In the login page, a client enters a username and password, which the switch forwards to a RADIUS server for authentication. After authenticating a client, the switch grants access to the secured network. Besides a web browser, the client needs no special supplicant software.

The **MAC Authentication (MAC-Auth)** method grants access to a secure network by authenticating devices for access to the network. When a device connects to the switch, either by direct link or through the network, the switch forwards the device’s MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the username and password, and grants or denies network access in the same way that it does for

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

clients capable of interactive logons. (The process does not use either a client device configuration or a logon session.) MAC authentication is well-suited for clients that are not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC-Auth to “lock” a particular device to a specific switch and port.

802.1X port-access, Web authentication, and MAC authentication can be configured at the same time on the same port. A maximum of 32 clients is supported on the port. (The default is one client.)

Note: 802.1X and RADIUS server are external and not included in this evaluation.

Dynamic IP Lockdown

The Dynamic IP Lockdown feature is used to prevent IP source address spoofing on a per-port and per-VLAN basis. When dynamic IP lockdown is enabled, IP packets in VLAN traffic received on a port are forwarded only if they contain a known source IP address and MAC address binding for the port. The IP-to-MAC address binding can either be statically configured or learned by the DHCP Snooping feature (pre-requisite).

DHCP snooping is used to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing the organization to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded.

Dynamic IP lockdown uses information collected in the DHCP Snooping lease database (outside scope) and through statically configured IP source bindings to create internal, per-port lists. The internal lists are dynamically created from known IP-to-MAC address bindings to filter VLAN traffic on both the source IP address and source MAC address.

Enabling DHCP snooping

DHCP snooping on VLANs is disabled by default. To enable DHCP snooping on a VLAN or range of VLANs enter this command:

```
HP_switch(config)# dhcp-snooping vlan <vlan-id-range>
```

Enabling Dynamic IP Lockdown

To enable dynamic IP lockdown on all ports or specified ports, enter the **ip source-lockdown** command at the global configuration level. Use the **no** form of the command to disable dynamic IP lockdown.

Syntax: [no] ip source-lockdown <port-list>

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Enables dynamic IP lockdown globally on all ports or on specified ports on the routing switch

Adding a Static Binding

To add the static configuration of an IP-to-MAC binding for a port to the lease database, enter the **ip source-binding** command at the global configuration level. Use the **no** form of the command to remove the IP-to-MAC binding from the database.

Syntax: [no] ip source-binding <vlan-id> <ip-address> <mac-address> <portnumber>

MAC Lockout

MAC Lockout involves configuring a MAC address on all ports and VLANs for a switch so that any traffic to or from the “locked-out” MAC address will be dropped. This means that all data packets addressed to or from the given address are stopped by the switch. MAC Lockout is implemented on a per switch assignment.

Think of MAC Lockout as a simple blacklist. The MAC address is locked out on the switch and on all VLANs. No data goes out or in from the blacklisted MAC address to a switch using MAC Lockout.

To fully lock out a MAC address from the network it would be necessary to use the MAC Lockout command on all switches.

To use MAC Lockout you must first know the MAC Address you wish to block.

Syntax: [no] lockout-mac < mac-address >

Let's say a customer knows there are unauthorized wireless clients who should not have access to the network. The network administrator “locks out” the MAC addresses for the wireless clients by using the MAC Lockout command (**lockout-mac <mac-address>**). When the wireless clients then attempt to use the network, the switch recognizes the intruding MAC addresses and prevents them from sending or receiving data on that network.

If a particular MAC address can be identified as unwanted on the switch then that MAC Address can be disallowed on all ports on that switch with a single command. You don't have to configure every single port—just perform the command on the switch and it is effective for all ports.

MAC Lockout is independent of port-security and in fact will override it. MAC Lockout is preferable to port-security to stop access from known devices because it can be configured for all ports on the switch with one command.

It is possible to use MAC Lockout in conjunction with port-security. You can use MAC Lockout to lock out a single address—deny access to a specific device—but still allow the switch some flexibility in learning other MAC Addresses.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

MAC Lockdown

MAC Lockdown, also known as “static addressing,” is the permanent assignment of a given MAC address (and VLAN, or Virtual Local Area Network) to a specific port on the switch. MAC Lockdown is used to prevent station movement and MAC address hijacking. It also controls address learning on the switch. When configured, the MAC Address can only be used on the assigned port and the client device will only be allowed on the assigned VLAN.

Port security and MAC Lockdown are mutually exclusive on a given port. You can either use port security or MAC Lockdown, but never both at the same time on the same port.

Syntax: [no] static-mac < *mac-addr* > vlan < *vid* > interface < *port-number* >

When a device’s MAC address is locked down to a port (typically in a pair with a VLAN) all information sent to that MAC address must go through the locked-down port. If the device is moved to another port it cannot receive data. Traffic to the designated MAC address goes only to the allowed port, whether the device is connected to it or not.

MAC Lockdown is useful for preventing an intruder from “hijacking” a MAC address from a known user in order to steal data. Without MAC Lockdown, this will cause the switch to learn the address on the malicious user’s port, allowing the intruder to steal the traffic meant for the legitimate user.

MAC Lockdown ensures that traffic intended for a specific MAC address can only go through the one port which is supposed to be connected to that MAC address. It does not prevent intruders from transmitting packets with the locked MAC address, but it does prevent responses to those packets from going anywhere other than the locked-down port. Thus TCP connections cannot be established. Traffic sent to the locked address cannot be hijacked and directed out the port of the intruder.

If the device (computer, PDA, wireless device) is moved to a different port on the switch (by reconnecting the Ethernet cable or by moving the device to an area using a wireless access point connected to a different port on that same switch), the port will detect that the MAC Address is not on the appropriate port and will continue to send traffic out the port to which the address was locked.

Once a MAC address is configured for one port, you cannot perform port security using the same MAC address on any other port on that same switch.

You cannot lock down a single MAC Address/VLAN pair to more than one port; however you can lock down multiple different MAC Addresses to a single port on the same switch.

Stations can move from the port to which their MAC address is locked to other parts of the network. They can send, but will not receive data if that data must go through the locked down switch. Please note that if the device moves to a distant part of the network where data sent to its MAC address never goes through the locked down switch, it may be possible for the device to have full two-way communication. For full and complete lockdown network-wide all switches must be configured appropriately.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Port Security

This feature enables you to configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

Basic Operation

Default Port Security Operation: The default port security setting for each port is off, or “continuous”. That is, any device can access a port without causing a security reaction.

Intruder Protection: A port that detects an “intruder” blocks the intruding device from transmitting to the network through that port.

Eavesdrop Protection: Using either the port-security command or the switch’s web browser interface to enable port security on a given port automatically enables eavesdrop prevention on that port.

General Operation for Port Security: On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once port security is configured, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as PCM and PCM+
- Alert Log entries in the switch’s web browser interface
- Event Log entries in the console interface
- Intrusion Log entries in the menu interface, CLI, or web browser interface

For any port, you can configure the following:

Action: Used when a port detects an intruder. Specifies whether to send an SNMP trap to a network management station (outside the TOE) and whether to disable the port.

Address Limit: Sets the number of authorized MAC addresses allowed on the port.

Learn-Mode: Specify how the port acquires authorized addresses.

- **Continuous:** Allows the port to learn addresses from inbound traffic from any connected device. This is the default setting.
- **Limited-Continuous:** Sets a finite limit (1 -32) to the number of learned addresses allowed per port.
- **Static:** Enables you to set a fixed limit on the number of MAC addresses authorized for the port and to specify some or all of the authorized addresses. (If you specify only some of the authorized addresses, the port learns the remaining authorized addresses from the traffic it receives from connected devices.)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- **Configured:** Requires that you specify all MAC addresses authorized for the port. The port is not allowed to learn addresses from inbound traffic.

Authorized (MAC) Addresses: Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:

- Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
- Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port. (For more on configuring the switch for SNMP management, see “Trap Receivers and Authentication Traps” in the Management and Configuration Guide for your switch.)

Port Access: Allows only the MAC address of a device authenticated through the switch’s 802.1X Port-Based access control.

Syntax: [no] port-security <port-list>< learn-mode | address-limit | mac-address | action | clear-intrusion-flag > learn-mode < continuous | static | port-access | configured | limited-continuous >

< **port-list** > - Specifies a list of one or more ports to which the port-security command applies.

learn-mode - Identifies the method for acquiring authorized addresses for the specified port.

On switches covered in this ST, this command automatically invokes eavesdrop protection.

Eavesdrop Prevention

Configuring port security on a given switch port automatically enables Eavesdrop Prevention for that port. This prevents use of the port to flood unicast packets addressed to MAC addresses unknown to the switch and blocks unauthorized users from eavesdropping on traffic intended for addresses that have aged-out of the switch’s address table. (Eavesdrop Prevention does not affect multicast and broadcast traffic; the switch floods these two traffic types out a given port regardless of whether port security is enabled on that port.)

Feature Interactions When Eavesdrop Prevention is Disabled

The following table explains the various interactions between learning modes and Eavesdrop Prevention when Eavesdrop Prevention is disabled.

When the learning mode is “port-access”, Eavesdrop Prevention will not be applied to the port. However, it can still be configured or disabled for the port.

Table 7-3: Learning Modes

Learn Mode	Effect
------------	--------

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Static	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured and only a limited number of static MAC addresses are learned. A device must generate traffic before the MAC address is learned and traffic is forwarded to it.
Continuous	The default. The Eavesdrop Prevention option does not apply because port security is disabled. Ports forward traffic with unknown destination addresses normally.
Port-access	Disabling Eavesdrop Prevention is not applied to the port. There is no change.
Limited-continuous	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured; MAC addresses age normally. Eavesdrop Prevention may cause difficulties in learning MAC addresses (as with static MAC addresses) and cause serious traffic issues when a MAC ages out.
Configured	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured by a static MAC address. Eavesdrop Prevention should not cause any issues because all valid MAC addresses have been configured.

Syntax: [no] port-security <port-list> eavesdrop-prevention

When this option is enabled, the port is prevented from transmitting packets that have unknown destination addresses. Only devices attached to the port receive packets intended for them. This option does not apply to a learning mode of port-access or continuous. (The default is enabled)

7.1.3.3 IFC-3 Protocol Rate Limiting Security Policy

(FDP_IFC.1 (3), FDP_IFF.1 (3), FMT_MSA.1, FMT_MSA.3)

All Traffic Rate-Limiting

Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. The rate limits for each direction of traffic flow on the same port are configured separately and the specified limits can be different.

When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port, and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks.

Rate-limiting is applied to the available bandwidth on a port, and not to any Rate-Limiting specific applications running through the port. If the total bandwidth requested by all applications is less than the configured maximum rate, then no rate-limit can be applied.

Rate-limiting is intended for use on edge ports in a network. It is not recommended for use on links to other switches, routers, or servers within a network, or for use in the network core. Doing so can interfere with applications the network requires to function properly. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

The **rate-limit all** command controls the rate of traffic sent or received on a port by setting a limit on the bandwidth available. It includes options for:

- Rate-limiting on either inbound or outbound traffic.
- Specifying the traffic rate as either a percentage of bandwidth, or in terms of bits per second.

Syntax: [no] int <port-list> rate-limit all < in | out > <percent <0-100> | kbps < 0-10000000>>

Configures a traffic rate limit (on non-trunked ports) on the link. The “no” form of the command disables rate-limiting on the specified ports. (The default is disabled.)

Options include:

in or **out** — Specifies a traffic rate limit on inbound traffic passing through that port, or on outbound traffic.

percent or **kbps** — Specifies the rate limit as a percentage of total available bandwidth, or in kilobits per second.

Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, Networking recommends using the **<port-list> disable** command instead of configuring a rate limit of 0.

The rate limit can be configured for/from either the global configuration level or from the port context level. For example, either of the following commands configures an inbound rate limit of 60% on ports A3 - A5:

HP_switch (config)# int a3-a5 rate-limit all in percent 60 → *Global*

HP_switch (eth-A3-A5)# rate-limit all in percent 60 → *Contextual*

ICMP Rate-Limiting

In IP networks, ICMP (Internet Control Message Protocol) messages are generated in response to either inquiries or requests from routing and diagnostic functions. These messages are directed to the applications originating the inquiries. In unusual situations, if the messages are generated rapidly with the intent of overloading network circuits, they can threaten network availability. This problem is visible in denial-of-service (DoS) attacks or other malicious behaviors where a worm or virus overloads the network with ICMP messages to an extent where no other traffic can get through. (ICMP messages themselves can also be misused as virus carriers). Such malicious misuses of ICMP can include a high number of ping packets that mimic a valid source IP address and an invalid destination IP address (spoofed pings), and a high number of response messages (such as Destination Unreachable error messages) generated by the network.

ICMP rate-limiting provides a method for limiting the amount of bandwidth that may be utilized for inbound ICMP traffic on a switch port or trunk. This feature allows users to restrict ICMP

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

traffic to percentage levels that permit necessary ICMP functions, but throttle additional traffic that may be due to worms or viruses (reducing their spread and effect). In addition, ICMP rate-limiting preserves inbound port bandwidth for non-ICMP traffic.

ICMP rate-limiting does not throttle non-ICMP traffic. In cases where both ICMP traffic and all other inbound traffic on a given interface need to be throttled the TOE provides the manager with the ability to separately configure both ICMP rate-limiting and all-traffic rate-limiting.

The all-traffic rate-limiting command (**rate-limit all**) and the ICMP rate-limiting command (**rate-limit icmp**) operate differently:

- All traffic rate-limiting applies to both inbound and outbound traffic, and can be specified either in terms of a percentage of total bandwidth or in terms of bits per second;
- ICMP rate-limiting applies only to inbound traffic, and can only be specified as a percentage of total bandwidth.

The **rate-limit icmp** command controls inbound usage of a port by setting a limit on the bandwidth available for inbound ICMP traffic.

Syntax: [no] int < port- list > rate-limit icmp <percent < 0-100 > | kbps <0-10000000>>

Configures inbound ICMP traffic rate limiting. You can configure a rate limit from either the global configuration level (as shown above) or from the interface context level. The **no** form of the command disables ICMP rate-limiting on the specified interface(s). (The default is disabled)

percent <1-100> - Values in this range allow ICMP traffic as a percentage of the bandwidth available on the interface.

kbps <0-10000000> - Specifies the rate at which to forward traffic in kilobits per second.

Configuring a rate limit of 0 (zero) causes an interface to drop all incoming ICMP traffic, and is not recommended.

For example, either of the following commands configures an inbound rate limit of 1% on ports A3 - A5, which are used as network edge ports:

HP_switch(config)# int a3-a5 rate-limit icmp 1 → **Global**

HP_switch (eth-A3-A5)# rate-limit icmp 1 → **Contextual**

Using Both ICMP Rate-Limiting and All-Traffic Rate-Limiting on the Same Interface

ICMP and all-traffic rate-limiting can be configured on the same interface. All-traffic rate-limiting applies to all inbound or outbound traffic (including ICMP traffic), while ICMP rate-limiting applies only to inbound ICMP traffic.

Please note that if the all-traffic load on an interface meets or exceeds the currently configured all-traffic inbound rate-limit while the ICMP traffic rate-limit on the same interface has not been

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

reached, then all excess traffic will be dropped, including any inbound ICMP traffic above the all-traffic limit (regardless of whether the ICMP rate-limit has been reached). Suppose, for example:

- The all-traffic inbound rate-limit on port “X” is configured at 55% of the port’s bandwidth.
- The ICMP traffic rate-limit on port “X” is configured at 2% of the port’s bandwidth.

If at a given moment:

- Inbound ICMP traffic on port “X” is using 1% of the port’s bandwidth, and
- Inbound traffic of all types on port “X” demands 61% of the port’s bandwidth,

then all inbound traffic above 55% of the port’s bandwidth, including any additional ICMP traffic, will be dropped as long as all inbound traffic combined on the port demands 55% or more of the port’s bandwidth.

7.1.3.4 IFC-4 Port and Protocol Filtering Security Policy

(FDP_IFC.1 (4), FDP_IFF.1 (4), FMT_MSA.1, FMT_MSA.3)

The TOE support the ability to configure a traffic filter to either forward or drop all network traffic moving to outbound (destination) ports and trunks (if any) on the switch.

Filter Limits

The switch accepts up to 101 static filters. These limitations apply:

- Source-port filters: up to 78
- Multicast filters: up to 16 with 1024 or fewer VLANs configured. Up to 8 with more than 1024 VLANs configured.
- Protocol filters: up to 7

Filter Types and Operations

- Source-Port: Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.
- Multicast: Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports (the default) or dropped on a per-port (destination) basis.
- Protocol: Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.

Each source-port filter includes:

- One source port or port trunk (**trk1, trk2 ...trkN**)
- A set of destination ports and/or port trunks that includes all untrunked LAN ports and port trunks on the switch

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- An action (forward or drop) for each destination port or port trunk

When a source-port filter created, the switch automatically sets the filter to forward traffic from the designated source to all destinations for which the manager does not specifically configure a “drop” action. Thus, it is not necessary to configure a source-port filter for traffic that is desired to be forward unless the filter was previously configured to drop the desired traffic.

Packets allowed for forwarding by a source-port filter are subject to the same operation as inbound packets on a port that is not configured for source-port filtering.

Syntax: [no] filter [source-port < port-number | trunk-name>]
[drop] < destination-port-list > [forward < port-list >] [forward < port-list>]

Example of Creating a Source-Port Filter:

For example, assume that there is a need to create a source-port filter that drops all traffic received on port 5 with a destination of port trunk 1 (Trk1) and any port in the range of port 10 to port 15. To create this filter execute this command:

```
HP_switch(config)# filter source-port 5 drop trk1,10-15
```

Static Multicast Filters

This filter type enables the switch to forward or drop multicast traffic to a specific set of destination ports. This helps to preserve bandwidth by reducing multicast traffic on ports where it is unnecessary, and to isolate multicast traffic to enhance security.

You can up to 16 static multicast filters (defined by the **filter** command) can be configured. However, if an IGMP-controlled filter for a joined multicast group has the same multicast address as a static multicast filter configured on a given port, the IGMP-controlled filter overrides the static multicast filter configured on that port.

Note: In the default configuration, IGMP is disabled on VLANs configured in the switch.

To enable IGMP on a specific VLAN, use the **vlan < vid > ip igmp** command. (

The total of static multicast filters and IGMP multicast filters together can range from 389 to 420, depending on the current **max-vlans** setting in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

Syntax: [no] filter [multicast < mac-address >] [< forward | drop > < port-list >]

Protocol Filters

This filter type enables the switch to forward or drop, on the basis of protocol type, traffic to a specific set of destination ports on the switch. Filtered protocol types include:

- AppleTalk
- NetBEUI

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- ARP
- SNA
- IPX

Only one filter for a particular protocol type can be configured at any one time. For example, a separate protocol filter can be configured for each of the protocol types listed above, but only one of those can be an IP filter. Also, the destination ports for a protocol filter can be on different VLANs.

Up to seven protocol filters can be configured.

Syntax: [no] filter [protocol < ip | ipx | arp | appletalk | sna | netbeui >]
[< forward | drop > < *port-list* >]

DHCP snooping

DHCP snooping is used to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing the organization to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded.

Dynamic IP lockdown uses information collected in the DHCP Snooping lease database (outside scope) and through statically configured IP source bindings to create internal, per-port lists. The internal lists are dynamically created from known IP-to-MAC address bindings to filter VLAN traffic on both the source IP address and source MAC address.

Enabling DHCP snooping

DHCP snooping on VLANs is disabled by default. To enable DHCP snooping on a VLAN or range of VLANs enter this command:

Syntax: [no] dhcp-snooping [authorized-server | database | option | trust | verify | vlan]

authorized server - Enter the IP address of a trusted DHCP server. If no authorized servers are configured, all DHCP server addresses are considered valid. Maximum: 20 authorized servers

database - To configure a location for the lease database, enter a URL in the format **ftp://ip-addr/ascii-string**. The maximum number of characters for the URL is 63.

option - Add relay information option (Option 82) to DHCP client packets that are being forwarded out trusted ports. The default is yes, add relay information.

trust - Configure trusted ports. Only server packets received on trusted ports are forwarded. The default is untrusted

verify - Enables DHCP packet validation. The DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or the packet is dropped. Default: **Yes**

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

vlan - Enable DHCP snooping on a vlan. DHCP snooping must be enabled already. The default is no.

7.1.3.5 IFC-5 ACL Filtering Security Policy

An ACL is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criteria and an action (permit or deny). A static ACL applies only to the switch in which it is configured. ACLs operate on assigned interfaces, and offer these traffic filtering options:

- IPv4 traffic inbound on a port.
- IPv4 traffic inbound on a VLAN.
- Routed IPv4 traffic entering or leaving the switch on a VLAN.

Note: ACLs do not screen traffic at the internal point where traffic moves between VLANs or subnets within the switch.

Types of IPv4 ACLs

A permit or deny policy for IPv4 traffic you want to filter can be based on source address alone, or on source address plus other factors.

Standard ACL: Standard ACLs permit or deny IPv4 traffic based on source address only. Standard ACLs are also useful to quickly control a performance problem by limiting IPv4 traffic from a subnet, group of devices, or a single device. (This can block all IPv4 traffic from the configured source, but does not hamper IPv4 traffic from other sources within the network.) A standard ACL uses an alphanumeric ID string or a numeric ID of 1 through 99. A single host, a finite group of hosts, or any host can be specified

Standard ACL Attributes: Uses only a packet's source IPv4 address as a criterion for permitting or denying the packet.

Extended ACL: An extended ACL permits or denies IPv4 traffic based on source address, destination address, combination of source and destination address, and IPv4 protocol options such as TCP applications (Telnet, http, ftp, and others).

Extended ACL attributes: Offers the following criteria as options for permitting or denying a packet:

- Source IPv4 address
- Destination IPv4 address
- IPv4 protocol options:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Any IPv4 traffic
- Any traffic of a specific IPv4 protocol type (0-255)
- Any TCP traffic (only) for a specific TCP port or range of ports, including optional use of TCP control bits or control of connection (established) traffic based on whether the initial request should be allowed
- Any UDP traffic (only) or UDP traffic for a specific UDP port
- Any ICMP traffic (only) or ICMP traffic of a specific type and code
- Any IGMP traffic (only) or IGMP traffic of a specific type
- Any of the above with specific precedence and/or ToS settings

Access Control Entry (ACE): A policy entry consisting of the criteria (policy attributes) and the action (permit or deny) to be executed on a packet if it meets the criteria. The elements composing the criteria include:

- source IPv4 address and mask (standard and extended ACLs)
- destination IPv4 address and mask (extended ACLs only)
- either of the following:
 - all IPv4 traffic
 - IPv4 traffic of a specific IP protocol (extended ACLs only) (In the cases of TCP, UDP, ICMP, and IGMP, the criteria can include either all traffic of the protocol type or only the traffic of a specific sub-type within the protocol.)
- option to log packet matches with deny ACEs
- optional use of IP precedence and ToS settings (extended ACLs only)

ACL Applications

The following table lists the range of interface options:

Table 7-4: Interface Options

Interface	ACL Application	Application Point	Filter Action
Port	Static Port ACL (switch configured)	inbound on the switch port	inbound IPv4 traffic
	RADIUS-Assigned ACL	inbound on the switch port used by authenticated client	inbound IPv4 and/or IPv6 traffic from the authenticated client

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

VLAN	VACL	entering the switch on the VLAN	inbound IPv4 traffic
	RACL	entering the switch on the VLAN	routed IPv4 traffic entering the switch and any IPv4 traffic with a destination on the switch itself
		exiting from the switch on the VLAN	routed IPv4 traffic exiting from the switch

When the switch uses an ACL to determine whether to permit or deny a packet, it compares the packet to the criteria specified in the individual Access Control Entries (ACEs) in the ACL, beginning with the first ACE in the list and proceeding sequentially until a match is found. When a match is found, the switch applies the indicated action (permit or deny) to the packet. This is significant because, once a match is found for a packet, subsequent ACEs in the same ACL will not be applied to that packet, regardless of whether they match the packet.

Allowing for the Implied Deny Function

In any ACL having one or more ACEs there will always be a packet match. This is because the switch automatically applies an Implicit Deny as the last ACE in any ACL. This function is not visible in ACL listings, but is always present. This means that if the switch is configured to use an ACL for filtering either inbound or outbound IPv4 traffic on a VLAN, any packets not specifically permitted or denied by the explicit entries will be denied by the Implicit Deny action. The Implicit Deny can be preempted (so that IPv4 traffic not specifically addressed by earlier ACEs in a given ACL will be permitted), insert an explicit **permit any** (for standard ACLs) or **permit ip any** (for extended ACLs) as the last explicit ACE in the ACL.

A Configured ACL Has No Effect Until You Apply It to an Interface

The switch stores ACLs in the configuration file. Thus, until you actually assign an ACL to an interface, it is present in the configuration, but not used.

Two special applications for ACL application is for routed traffic (RACL) and for a VLAN (VACL).

VACL Applications

VACLs filter any IPv4 traffic entering the switch on a VLAN configured with the "VLAN" ACL option.

```
vlan < vid > ip access-group < identifier > vlan
```

For example, an administrator could assign a VACL to VLAN 2 to filter all inbound switched or routed IPv4 traffic received from clients on the 10.28.20.0 network. In this instance, routed traffic received on VLAN 2 from VLANs 1 or 3 would not be filtered by the VACL on VLAN 2.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

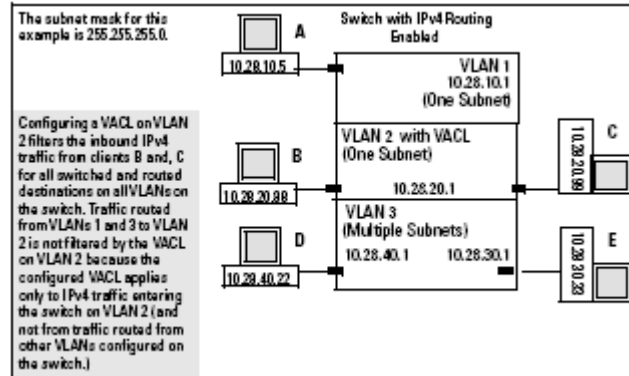


Figure 10: Example of VACL Filter Application to IPv4 Traffic Entering the Switch

The switch allows one VACL assignment configured per VLAN. This is in addition to any other ACL applications assigned to the VLAN or to ports in the VLAN.

RACL Applications

RACLs filter routed IPv4 traffic entering or leaving the switch on VLANs configured with the “in” and/or “out” ACL option

```
vlan < vid > ip access-group < identifier > < in | out >
```

For example, in the following figure:

An administrator could assign either an inbound ACL on VLAN 1 or an outbound ACL on VLAN 2 to filter a packet routed between subnets on different VLANs; that is, from the workstation 10.28.10.5 on VLAN 1 to the server at 10.28.20.99 on VLAN 2. (An outbound ACL on VLAN 1 or an inbound ACL on VLAN 2 would not filter the packet.)

Where multiple subnets are configured on the same VLAN, either inbound or outbound ACLs to filter routed IPv4 traffic between the subnets on the VLAN. (Traffic source and destination IP addresses must be on devices external to the switch.)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

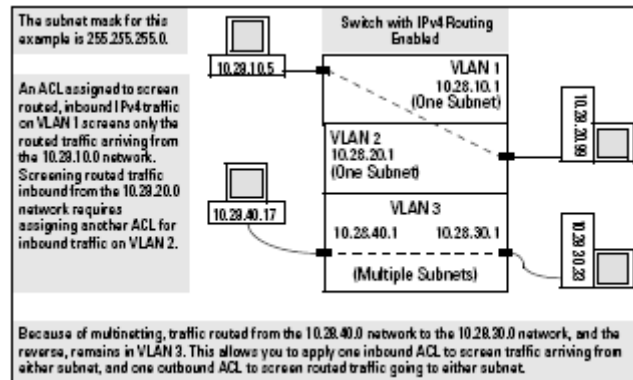


Figure 11: Example of RACL Filter Applications on Routed IPv4 Traffic

The switch allows one inbound RACL assignment and one outbound RACL assignment configured per VLAN. This is in addition to any other ACL assigned to the VLAN or to any ports on the VLAN. You can use the same RACL or different RACLs to filter inbound and outbound routed traffic on a VLAN.

RACLs do not filter IPv4 traffic that remains in the same subnet from source to destination (switched traffic) unless the destination address (DA) or source address (SA) is on the switch itself.

Practical Example

For a Packet To Be Permitted, It Must Have a Match with a “Permit” ACE in All Applicable ACLs Assigned to an Interface.

On a given interface where multiple ACLs apply to the same traffic, a packet having a match with a **deny** ACE in any applicable ACL on the interface (including an implicit **deny any**) will be dropped.

For example, suppose the following is true:

- Port A10 belongs to VLAN 100.
- A static port ACL is configured on port A10.
- A VACL is configured on VLAN 100.
- An RACL is also configured for inbound, routed traffic on VLAN 100.

An inbound, *switched* packet entering on port A10, with a destination on port A12, will be screened by the static port ACL and the VACL, regardless of a match with any **permit** or **deny** action. A match with a **deny** action (including an implicit **deny**) in either ACL will cause the switch to drop the packet. (If the packet has a match with explicit **deny** ACEs in multiple ACLs and the log option is included in these ACEs, then a separate log event will occur for each match.) The switched packet will not be screened by the RACL.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

However, suppose that VLAN 2 in figure below is configured with the following:

- A VACL permitting traffic having a destination on the 10.28.10.0 subnet
- An RACL that denies inbound traffic having a destination on the 10.28.10.0 subnet

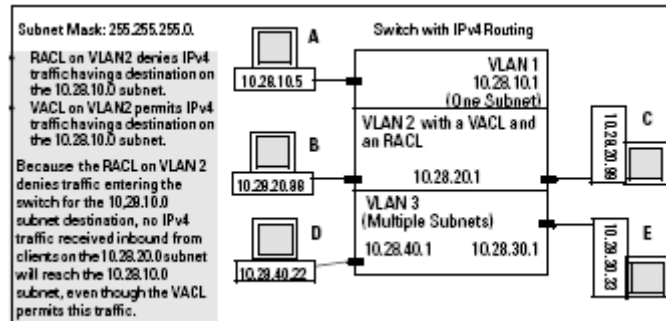


Figure 12 Example of Order of Application for Multiple ACLs on an Interface

In this case, no IPv4 traffic received on the switch from clients on the 10.28.20.0 subnet will reach the 10.28.10.0 subnet, even though the VACL allows such traffic. This is because the **deny** in the RACL causes the switch to drop the traffic regardless of whether any other VACLs permit the traffic.

7.1.4 Security Management with Access Control

7.1.4.1 SM-1: Management Functions

(FMT_SMF.1, FMT_MTD.1)

The TOE is capable of performing the security management functions as defined in Table 6-5: Management of TSF data. (See Section 6.1.5.3 FMT_MTD.1 Management of TSF data).

All management functions are limited to the administrative roles as defined in Section 7.1.4.2 SM-2: Management Security Roles below.

The management functions for the TOE are accessible through the Menu Interface, CLI, web browser interface, and physical front panel of switch.

Operational Environment Support

SM-1: Management Functions is supported by the Operational Environment through:

- Physical protection of switch

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- Network support for web browser interface

7.1.4.2 SM-2: Management Security Roles

(FMT_SMR.1, FMT_SMR.3)

There are two levels of access (roles): Manager and Operator for the Web Interface and Menu interface.

Each level has the following privileges/functionality available:

MENU INTERFACE

Operator Privilege: Access to the Status and Counters menu, the Event Log, and the CLI*, but no Configuration capabilities.

On the Operator level, the configuration menus, Download OS, and Reboot Switch options in the Main Menu are not available.

Manager Privilege: Access to all Menu interface areas.

This is the default level. That is, if a Manager password has not been set prior to starting the current console session, then anyone having access to the console can access any area of the console interface.

*Allows use of the ping, link-test, show, menu, exit, and logout commands, plus the enable command if the Manager password is provided.

WEB INTERFACE

Operator Setting: An Operator-level user name and password allows read-only access to most of the web browser interface, but prevents access to the Security window.

Manager Setting: A Manager-level user name and password allows full read/write access to the web browser interface.

CLI

There are 4 levels of access (roles): Operator, Manager, Global Configuration, and Context configuration for the CLI interface. The Global and Context configuration levels are hierarchical in that when a user logs in he or she must login as either Operator or Manager. If the user logs in as Operator then one must switch to Manger level, then switch to Global Configuration, and then switch to Context Configuration.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

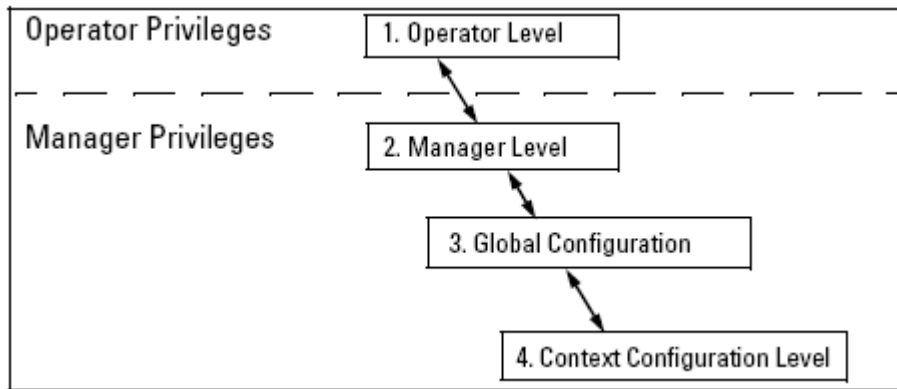


Figure 13: Access Sequence for Privilege Levels

Operator Privileges

At the Operator level a user can examine the current configuration and move between interfaces without being able to change the configuration. A “>” character delimits the Operator-level prompt. For example:

HP_switch> _ Example of the Operator prompt.

When using **enable** to move to the Manager level, the switch prompts for the Manager password if one has already been configured.

Manager Privileges

Manager privileges give three additional levels of access: Manager, Global Configuration, and Context Configuration. A “#” character delimits any Manager prompt. For example:

HP_switch# _ Example of the Manager prompt.

Manager level: Provides all Operator level privileges plus the ability to perform system-level actions that do not require saving changes to the system configuration file. The prompt for the Manager level contains only the system name and the “#” delimiter, as shown above. To select this level, enter the **enable** command at the Operator prompt and enter the Manager password, when prompted. For example:

HP_switch> enable Enter enable at the Operator prompt.

Password: CLI prompt for the Manager password.

HP_switch# _ The Manager prompt appears after the correct Manager password is entered.

Global Configuration

Global Configuration level: Provides all Operator and Manager level privileges, and enables configuration changes to any of the switch’s software features. The prompt for the Global

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Configuration level includes the system name and “(config)”. To select this level, enter the config command at the Manager prompt. For example:

HP_switch# config Enter **config** at the Manager prompt.

HP_switch(config)# The Global Config prompt.

Context Configuration

Context Configuration level: Provides all Operator and Manager privileges, and enables configuration changes in a specific context, such as one or more ports or a VLAN. The prompt for the Context Configuration level includes the system name and the selected context. For example:

HP_switch(eth-1)#

HP_switch(vlan-10)#

7.1.4.3 SM-3: Management Access Control

(FMT_MTD.1, FMT_SMR.1)

All users of the TOE have access (read or write) to management functions and/or TSF data as defined in Table 6-5: Management of TSF data. (See Section 6.1.5.3 FMT_MTD.1 Management of TSF data. Therefore, all TOE users are considered administrators.

Switch management access is available through the following methods:

- Front-Panel access (serial port access to the console, plus resets and clearing the password(s) or current configuration)
- Console serial port
- SNMPv3 access
- SSH access and Web-browser access

Management functions and operations are available through the following methods:

- **Menu interface**—a menu-driven interface offering a subset of switch commands through the built-in VT-100/ANSI console
- **CLI**—a command line interface offering the full set of switch commands through the VT-100/ANSI console built into the switch
- **Web browser interface** —a switch interface offering status information and a subset of switch commands through a standard web browser (such as Netscape Navigator or Microsoft Internet Explorer)

Front-Panel Access and Physical Security

Physical access to the switch allows the following:

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch's Clear and Reset buttons for these actions:
 - clearing (removing) local password protection
 - rebooting the switch
 - restoring the switch to the factory default configuration (and erasing any non-default configuration settings)

The switch must be locked in a wiring closet or other secure space to help prevent unauthorized physical access. The TOE provides the following capabilities that can be used to minimize the vulnerability of a person having physical access to the appliance:

- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset + Clear button combination so that the switch reboots, but does not restore the switch's factory default settings.
- Disable or re-enable password recovery.

Console Serial Port connection (Local Manager Password Protection)

In the default configuration, there is no password protection. Configuring a local Manager and Operator password is a fundamental step in reducing the possibility of unauthorized access through the switch's Web browser and console (CLI and Menu) interfaces. The Manager and Operator password can easily be set using the CLI ***password manager*** command, the Menu interface ***Console Passwords*** option, or the ***password*** options under the ***Security tab*** in the Web browser interface.

Note that the TOE provides no individual username accountability. Usernames may be associated with a Manager and/or Operator level (role), but are pseudo names for the particular roles. All human users that are assigned to be Operators for the switch use the same username (if it exists) and password combinations to access the switch. This would be the same for human users that have been assigned as Managers of the switch.

Based on the password entered, which is either associated with Manger or Operator role see Section 7.1.4.2 SM-2: Management Security Roles above), the TOE restricts access to the functions as defined in Table 6-5: Management of TSF data. (See Section 6.1.5.3 FMT_MTD.1 Management of TSF data).

SNMP Access

General SNMP Access to the Switch.

In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing and changing the settings and status

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

data in the switch's MIB (Management Information Base). Controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of any network security strategy.

The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options. CC evaluated configuration requires that SNMP version 3 be enabled if using this optional interface. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation).

SNMPv3 security options include:

- configuring device communities as a means for excluding management
- access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers
- restricting non-SNMPv3 agents to either read-only access or no access
 - (CLI command: **snmp-server mib hpswitchauthmib excluded**)
- co-existing with SNMPv1 and v2c if necessary

SNMP Access to the Authentication Configuration MIB.

Beginning with software release K.12.xx, a management station running an SNMP networked device management application, such as PCM+ or HP OpenView (neither of which are in scope), can access the switch's management information base (MIB) for read access to the switch's status and read/write access to the switch's authentication configuration (hpSwitchAuth). This means that the switch's default configuration now allows SNMP access to security settings in hpSwitchAuth.

If SNMP access to the hpSwitchAuth MIB is considered an unacceptable security risk for the target network, then the following security precautions should be implemented immediately after booting from software release K.12.xx or greater for the first time:

- use the following command to disable this feature:
 - **snmp-server mib hpswitchauthmib excluded**
- If accessibility is required for the authentication configuration MIB, then the following to needs to be implemented to help ensure that unauthorized workstations cannot use SNMP tools to access the MIB:
 - Configure SNMP version 3 management and access security on the switch.
 - Disable SNMP version 2c on the switch.

Inbound SSH Access and Web Browser Access

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

The default remote management protocols (enabled on the switch) are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing passwords, secure and encrypted protocols such as SSH and SSL must be used for remote access. This provides the capability to employ increased access security while still retaining remote client access.

- SSHv2 provides Telnet-like connections through encrypted and authenticated transactions.
- SSLv3/TLS(v1.0, 1.1, 1.2) provides remote Web browser access to the switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

Also, access security on the switch is incomplete without disabling Telnet and the standard Web browser access. Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two CLI commands:

- no telnet-server: This command blocks inbound Telnet access.
- no web-management: This command prevents use of the Web browser interface through http (port 80) server access.

For CC compliance Telnet and standard Web browser access must be disabled. To use remote management SSH and SSL must be used.

Other Provisions for Management Access Security

The following features can help to prevent unauthorized management access to the switch.

External Authorized IP Managers

This feature uses IP addresses and masks to determine whether to allow management access to the switch across the network through the following:

- SSH
- The switch's Web browser interface (SSL)
- SNMPv3

Secure Management VLAN

This feature creates an isolated network for managing the HP Networking Switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and Web browser interface access is restricted to ports configured as members of the VLAN.

External TACACS+ Authentication

.As previously described in IA-3 User Authentication, the TOE can be configured to invoke an external TACACS+ server for access control decisions. See IA-3 for details.

External RADIUS Authentication

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

As previously described in IA-3 User Authentication, the TOE can be configured to invoke an external RADIUS server for access control decisions. See IA-3 for details.

ACLs for Management Access Protection

ACLs can also be configured to protect management access by blocking inbound IP traffic that has the switch itself as the destination IP address.

7.1.5 TOE Access

7.1.5.1 TA-1: Login Banner

(FTA_TAB.1)

The switch can be configured to display a login banner of up to 3070 characters when an user initiates a management session with the switch through any of the following methods:

- serial connection
- SSHv2
- Web browser

The default banner displays product registration information.

If a banner is configured, the banner page is displayed when the Web user interface is accessed. The default product registration information is not displayed as there is already a product registration prompt displayed in the Web user interface.

Banner Operation with Serial, or SSHv2 Access

When a system operator begins a login session, the switch displays the banner above the local password prompt or, if no password is configured, above the **Press any key to continue prompt**. Entering a correct password or, if no password is configured, pressing any key clears the banner from the CLI and displays the CLI prompt.

Banner Operation with Web Browser Access

When a system operator uses a Web browser to access the switch, the text of a non-default banner configured on the switch appears in a dedicated banner window with a link to the Web agent home page. Clicking on **To Home Page** clears the banner window and prompts the user for a password (if configured).

Following entry of the correct username/password information (or if no username/password is required), the switch then displays either the Registration page or the switch's home page.

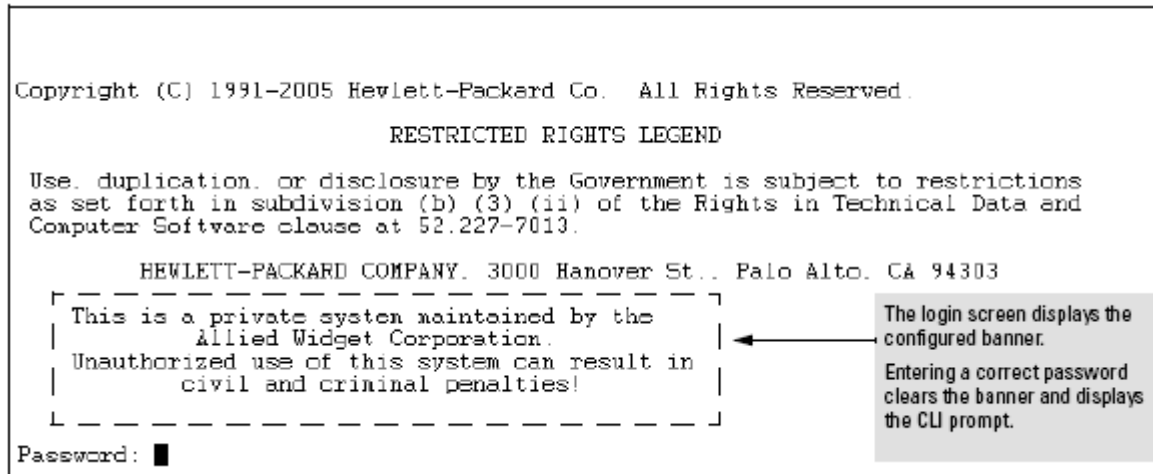
HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Note: If the banner feature is disabled or if the switch is using the factory-default banner, then the banner page does not appear in the Web browser when an operator initiates a login session with the switch.



```
Copyright (C) 1991-2005 Hewlett-Packard Co. All Rights Reserved.  
  
RESTRICTED RIGHTS LEGEND  
  
Use, duplication, or disclosure by the Government is subject to restrictions  
as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and  
Computer Software clause at 52.227-7013.  
  
HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303  
-----  
| This is a private system maintained by the Allied Widget Corporation. |  
| Unauthorized use of this system can result in civil and criminal penalties! |  
-----  
Password: █
```

The login screen displays the configured banner.
Entering a correct password clears the banner and displays the CLI prompt.

Figure 14: Example of CLI Result of the Login Banner Configuration

```
This is a private system maintained by the  
Allied Widget Corporation.  
Unauthorized use of this system can result in  
civil and criminal penalties!
```

[To Home Page](#)

Figure 15: Example of Web Browser Interface Result of the Login Banner

7.1.5.2 TA-2 Inactivity Termination

(FTA_SSL.3)

The TOE provides the capability to set an inactivity timeout. This causes the console session to end after the specified period of inactivity, thus giving added security against unauthorized console access.

The Manager can use either of the following to set the inactivity timer:

- Menu Interface: Select “2. Switch Configuration.
- CLI: Use the **console inactivity-timer < 0 | 1 | 5 | 10 | 15 | 20 | 30 | 60 | 120 >** where time is in minutes.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

7.1.6 Protection of TSF

7.1.6.1 TP-1: Cryptographic Support

(FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPT_ITC_EXP.1)

The TOE can generate the RSA and DSA keys defined Table 6-3: Cryptographic Support Parameters.

The keys are used to generate the server certificates which are stored in the switch's flash memory. The server certificate should be added to the certificate folder on the SSL clients who need to have access to the switch. Most browser applications automatically add the switch's host certificate to their certificate folder on the first use. This method does allow for a security breach on the first access to the switch.

There are two types of certificates that can be used for the switch's host certificate. The first type is a self-signed certificate, which is generated and digitally signed by the switch. Since self-signed certificates are not signed by a third-party certificate authority, there is no audit trail to a root CA certificate and no fool-proof means of verifying authenticity of certificate. The second type is a certificate authority-signed certificate, which is digitally signed by a certificate authority, has an audit trail to a root CA certificate, and can be verified unequivocally

To Generate or Erase the Switch's Public/Private Host Key Pair.

Syntax: crypto key generate <autorun-key [rsa] | cert [rsa] <keysize> | ssh [dsa | rsa] bits <keysize>>

Installs authentication files for ssh or https server, or for autorun.

autorun-key - Install RSA key for autorun.

cert - Install RSA key for https certificate.

ssh [dsa | rsa] - Install host key for ssh server. Specify the key type as DSA or RSA.

bits <keysize> - Specify the key size (in bits).

Syntax: zeroize <ssh | cert | autorun [rsa]>

Erases the switch's public/private key pair and disables SSH operation.

Syntax: show crypto host-public-key

Displays switch's public key. Displays the version 1 and version 2 views of the key.

Syntax: babble

Displays hashes of the switch's public key in phonetic format.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Syntax: fingerprint

Displays fingerprints of the switch's public key in hexadecimal format.

The encryption operations are defined in Table 6-4: Cryptographic Algorithms. Below is a summary of those ciphers used for the trusted communications for security management access.

The [no] **ip ssh** command allows the Manager to disable various specific cipher types to be used for the connection.

Valid cipher types for SSH are:

- aes128-cbc
- 3des-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes128-ctr
- aes192-ctr
- aes256-ctr

Default: All cipher types are available.

SSL supports the following preferred ciphers

- AES256_SHA
- AES128_SHA

There is no ability to disable a cipher type for SSL

SSH

The TOE uses Secure Shell version 2 (SSHv2) to provide remote access to management functions on the switches via encrypted paths between the switch and management station clients capable of SSH operation.

SSH provides Telnet-like functions but, unlike Telnet, SSH provides encrypted, authenticated transactions. The authentication types include:

- Client public-key authentication
- Switch SSH and user password authentication

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Client Public Key Authentication (Login/Operator Level) with User Password Authentication (Enable/Manager Level).

This option uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch. (The same private key can be stored on one or more clients.)

SSH in HP Networking Switches is based on the Mocana software toolkit.

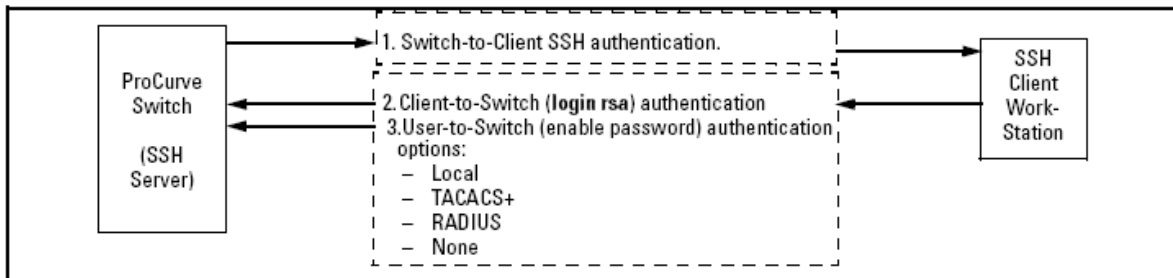


Figure 16: Client Public Key SSH Authentication Model

Switch SSH and User Password Authentication.

This option is a subset of the client public-key authentication. It occurs if the switch has SSH enabled but does not have login access (login public-key) configured to authenticate the client's key. The switch authenticates itself to SSH clients. Users on SSH clients then authenticate themselves to the switch (login and/or enable levels) by providing passwords stored locally on the switch or on a TACACS+ or RADIUS server. However, the client does not use a key to authenticate itself to the switch.

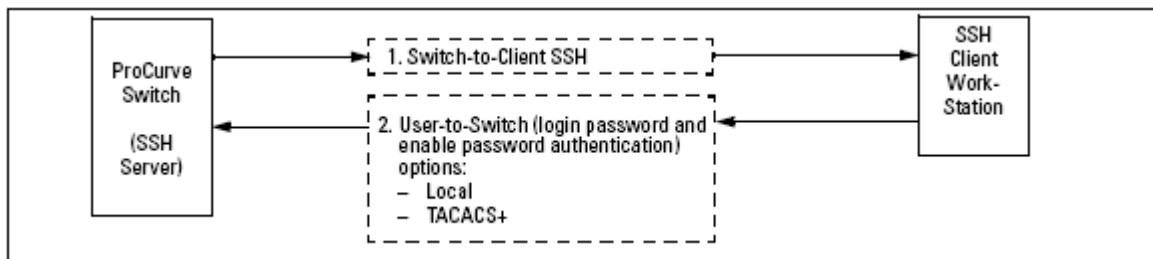


Figure 17: Switch/User SSH Authentication

HP Networking SSH Terminology

SSH Server: An HP Networking Switch with SSH enabled.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Key Pair: A pair of keys generated by the switch or an SSH client application. Each pair includes a public key, that can be read by anyone and a private key held internally in the switch or by a client.

PEM (Privacy Enhanced Mode): Refers to an ASCII-formatted client public-key that has been encoded for portability and efficiency. SSHv2 client public-keys are typically stored in the PEM format.

Private Key: An internally generated key used in the authentication process. A private key generated by the switch is not accessible for viewing or copying. A private key generated by an SSH client application is typically stored in a file on the client device and, together with its public key counterpart, can be copied and stored on multiple devices.

Public Key: An internally generated counterpart to a private key. A device's public key is used to authenticate the device to other devices.

Enable Level: Manager privileges on the switch.

Login Level: Operator privileges on the switch.

Local password or username: A Manager-level or Operator-level password configured in the switch.

SSH Enabled: (1) A public/private key pair has been generated on the switch (**generate ssh [dsa | rsa]**) and (2) SSH is enabled (**ip ssh**). (A key pair can be generated without enabling SSH, but SSH cannot be enabled without first generating a key pair.)

Prerequisite for Using SSH

Before using the switch as an SSH server, a publicly or commercially available SSH client application must be installed on the computer(s) that will be used for management access to the switch. If client public-key authentication is desired, then the client program must have the capability to generate or import keys.

Any client application used for client public-key authentication with the switch must have the capability to export public keys. The switch can accept keys in the PEM-Encoded ASCII Format or in the Non-Encoded ASCII format.

For two-way authentication between the switch and an SSH client, the login (Operator) level must be used.

Table 7-5: SSH Options

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Switch Access Level	Primary SSH Authentication	Authenticate Switch Public Key to SSH Clients?	Authenticate Client Public Key to the Switch?	Primary Switch Password Authentication	Secondary Switch Password Authentication
Operator (Login) Level	ssh login rsa	Yes	Yes ¹	No ¹	local or none
	ssh login Local	Yes	No	Yes	none
	ssh login TACACS	Yes	No	Yes	local or none
	ssh login RADIUS	Yes	No	Yes	local or none
Manager (Enable) Level	ssh enable local	Yes	No	Yes	none
	ssh enable tacacs	Yes	No	Yes	local or none
	ssh enable radius	Yes	No	Yes	local or none

¹ For **ssh login public-key**, the switch uses client public-key authentication instead of the switch password options for primary authentication.

SSL

The switches use Secure Socket Layer Version 3 (SSLv3) and support for Transport Layer Security (TLS versions 1.0, 1.1, 1.2) to provide remote web access to the switches via encrypted paths between the switch and management station clients capable of SSL/TLS operation. HP Networking Switches use SSL and TLS for all secure web transactions, and all references to SSL mean using one of these algorithms unless otherwise noted

SSL provides all the web functions but, unlike standard web access, SSL provides encrypted, authenticated transactions. The authentication type includes server certificate authentication with user password authentication.

SSL in the switches is based on the Mocana software toolkit.

Server Certificate authentication with User Password Authentication. This option is a subset of full certificate authentication of the user and host. It occurs only if the switch has SSL enabled. As in the figure below, the switch authenticates itself to SSL enabled web browser. Users on SSL browser then authenticate themselves to the switch (operator and/or manger levels) by providing passwords stored locally on the switch or on an external TACACS+ or RADIUS server (not included as part of the TOE).. However, the client does not use a certificate to authenticate itself to the switch.

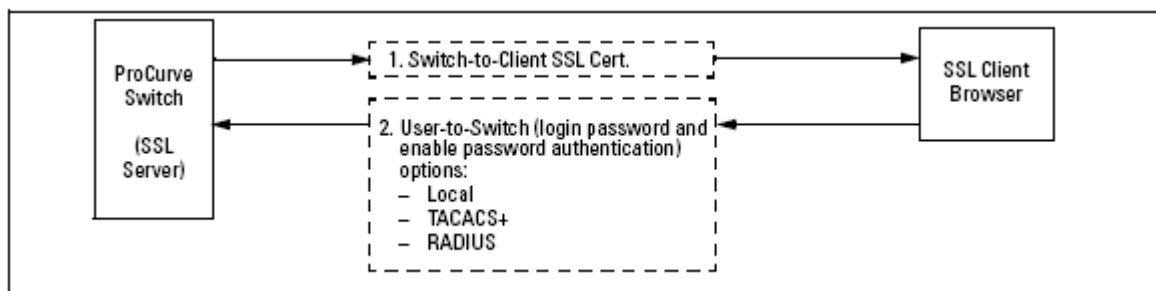


Figure 18: Switch/User SSL Authentication

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

SSL on the switches supports these preferred data encryption methods:

- AES256_SHA
- AES128_SHA

HP Networking Switches use RSA public key algorithms and Diffie-Hellman, and all references to a key mean keys generated using these algorithms unless otherwise noted

HP Networking SSL Terminology

SSL Server: An HP Networking Switch with SSL enabled.

Key Pair: Public/private pair of RSA keys generated by switch, of which public portion makes up part of server host certificate and private portion is stored in switch flash (not user accessible).

Digital Certificate: A certificate is an electronic “passport” that is used to establish the credentials of the subject to which the certificate was issued. Information contained within the certificate includes: name of the subject, serial number, date of validity, subject's public key, and the digital signature of the authority who issued the certificate. Certificates on HP Networking Switches conform to the X.509v3 standard, which defines the format of the certificate.

Self-Signed Certificate: A certificate not verified by a third-party certificate authority (CA). Self-signed certificates provide a reduced level of security compared to a CA-signed certificate.

CA-Signed Certificate: A certificate verified by a third party certificate authority (CA). Authenticity of CA-Signed certificates can be verified by an audit trail leading to a trusted root certificate.

Root Certificate: A trusted certificate used by certificate authorities to sign certificates (CA-Signed Certificates) and used later on to verify that authenticity of those signed certificates. Trusted certificates are distributed as an integral part of most popular web clients. (see browser documentation for which root certificates are pre-installed).

Manager Level: Manager privileges on the switch.

Operator Level: Operator privileges on the switch.

Local password or username: A Manager-level or Operator-level password configured in the switch.

SSL Enabled:

(1) A certificate key pair has been generated on the switch (web interface or CLI command: **crypto key generate cert [key size]**)

(2) A certificate been generated on the switch (web interface or CLI command: **crypto host-cert generate self-signed [arg-list]**) and (3) SSL is enabled (web interface or CLI command: **web-management ssl**). (A key pair can be generated without enabling SSL, but SSL cannot be enabled without first generating a key pair.)

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Prerequisite for Using SSL

Before using the switch as an SSL server, publicly or commercially available SSL enabled web browser application must be installed on the computer(s) used for management access to the switch.

Other support includes:

- SNMP version 3 which uses MD5 and/or SHA.

SNMPv3 User Commands

Syntax: [no] snmpv3 user <user_name>

Adds or deletes a user entry for SNMPv3. Authorization and privacy are optional, but to use privacy, authorization must be used. When a user is deleted, only the <user_name> is required.

[auth <md5 | sha> <auth_pass>]

With authorization, either MD5 or SHA authentication can be set. The authentication password <auth_pass> must be 6-32 characters in length and is mandatory when authentication is configured. The default is none.

[priv <des | aes> <priv_pass>]

With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption. The privacy password <priv_pass> must be 6-32 characters in length and is mandatory when privacy is configured. The default is DES.

Note: Only AES 128-bit and DES 56-bit encryption are supported as privacy protocols. Other non-standard encryption algorithms, such as AES-172, AES-256, and 3-DES are not supported.

- SNMP also uses MD5. The server is configured as SNMP Client Authentication Support.
 - The MD5 authentication mode must be selected.
 - An SNMP authentication key-identifier (key-id) must be configured on the switch and a value (key-value) must be provided for the authentication key. A maximum of 8 sets of key-id and key-value can be configured on the switch.
 - Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys will be used for SNMP authentication.
 - If the SNMP server requires authentication, one of the trusted keys has to be associated with the SNMP server.
 - SNMP client authentication must be enabled on the HP Networking Switch.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Operational Environment Support

TC-1: Trusted Communications is supported by the Operational Environment through:

- Network infrastructure
- TCP/IP protocols
- RADIUS server
- TACACS+ server
- SNMPv3
- SNTP Server

7.1.6.2 TP-2: Self Testing

(FPT_TST_EXP.1)

All products perform a self test to verify the correct operations of the hardware and software. The table below describes the test and the reaction the TSF takes upon the failure of a test category.

Table 7-6: Self Test Categories and Reactions

Test Category	If test fails, the following actions occur
Network transmission/reception tests	<ul style="list-style-type: none">• Switch operates but port is not usable• A log entry is made; a non-green led is lighted on the port
Inter-system communication tests	<ul style="list-style-type: none">• If interface module problem, then switch operates but interface module is not usable• If management module problem, then switch does not operate (see description below for further specific details about this test)
H/W infrastructure tests (LEDs, Fans, power supplies, temp. sensors, etc.)	<ul style="list-style-type: none">• If the power supply fails, the switch may report the error and continue if it has enough power, else the switch fails.• Fans, sensors, temp will indicate the failure in the log, but switch continues to work.• If a power supply is faulted an LED will light and a log entry will be made. Some blades may be powered off in the case of a 12 slot chassis, or fail to boot.
Memory tests (RAM, Flash, EEPROM)	<ul style="list-style-type: none">• Switch does not operate
ASIC tests (including internal logic blocks)	<ul style="list-style-type: none">• Switch does not operate
Power over Ethernet (PoE and controller) tests	<ul style="list-style-type: none">• PoE power will not be provided over that port, or block of ports, serviced by that controller;• network traffic over port should not be affected
USB tests	<ul style="list-style-type: none">• Switch operates but USB not usable.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

All switches have a management processor. In the chassis models (8200, 5400) this management hardware is removable/replaceable; in the stackable models (6600, 6200, 3500) this hardware is built-in and not customer replaceable.

The 8200zl models support Management processor redundancy. When the this switch boots up, the management modules run selftest routines to determine which module becomes the active management module and which becomes the standby management module. The module that was last active in the chassis is given precedence and becomes the “active” module. This module will be the one that is booted going forward. If a module fails selftest and is unable to communicate with the other module, it does not take control as the management module. The other management module will take control and become the active module. If both modules fail selftest, the fault LED flashes and neither module is operational.

The management boot decision process works as follows:

1. If there is only one management module, that is the active management module.
2. If one module is already booted and operational, a newly inserted module or the other management module booting will always become the standby module. The standby module does not become active unless a switchover occurs.
3. If there are two management modules and one fails selftest, the one that passes selftest becomes the active management module (switchover)
4. If there is only one management module and fails selftest, the switch fails to boot.
5. If there are two modules and both fail selftest the switch fails to boot.
6. If only one of two modules was ever booted in the chassis, that module is given precedence.
7. The module that was active on the last boot becomes the active management module. This guarantees that the active module has the latest configuration data.
8. If both management modules have previously booted in this chassis and were “active” the last time booted, the module that booted most recently becomes the active management module.
9. If none of the above conditions are applicable, the module in the lowest slot becomes the active management module.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

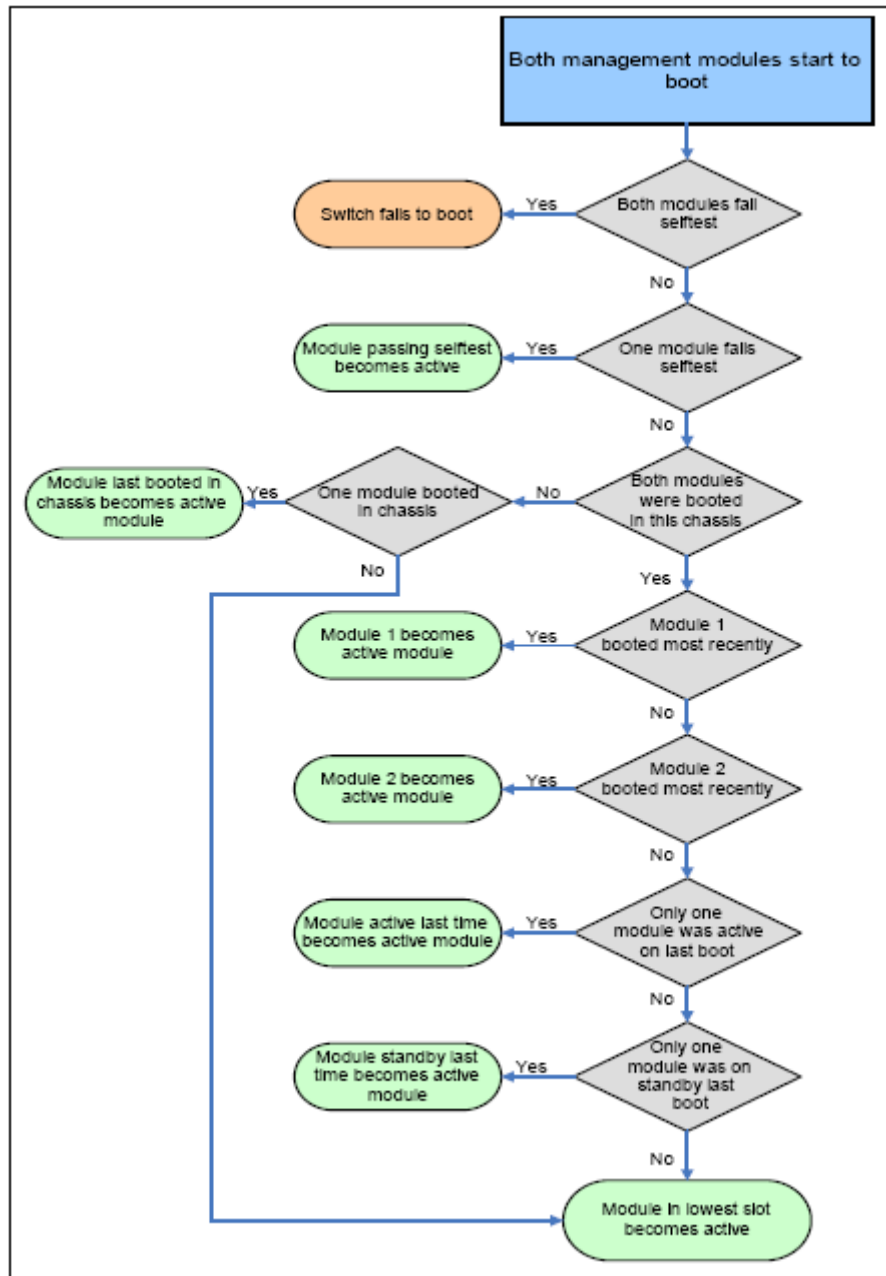


Figure 19: Management Module Self test Boot Process Flow Chart

Terminology

Redundant management uses the following terminology.

HP Network Switch

Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.09.04

Models: 3800 with Software Version KA.15.09.04

Security Target

Active Management Module. A management module that booted successfully and is actively managing the switch.

Standby Management Module. A management module that is ready to become the active management module if the active management module fails.

Failed Management Module. A management module that did not pass selftest and is not in standby mode.

Offline Management Module. A management module that is offline because redundancy is disabled.

Selftest. A test performed at boot to ensure the management module is functioning correctly. If the module fails selftest, it does not go into active or standby mode. If both modules fail selftest, the switch does not boot.

Switchover. When the other management module becomes the active management module.