Huawei CloudEngine Series Switch
V100R002
Security Target

Version: 0.8
Last Update: 2013-11-13
Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2013-05-20	0.1	Initial Draft	Huang Guodong,Li Wen
2013-07-17	0.2	Update according to review	Huang Guodong,Li Wen
2013-07-24	0.3	Updated FCS sections:	Satish karunanithi 71076,
2013-07-25	0.4	Review and update	Syed ajim hussain 70531 (Reviewed the document)
2013-09-06	0.5	Updated ST extensively to align with S-Switches ST	Jason Chen (Brightsight)
2013-10-01	0.6	Updated based on Huawei comments	Jason Chen (Brightsight)
2013-10-30	0.7	Updated based on Brightsight comments	Huang Guodong, Ramu N 00900652
2013-11-13	0.8	Updated based on Brightsight comments	Huang Guodong, Manish Patidar 70964, Li Wen

Table of Contents

TABLE OF CONTENTS **3**
LIST OF TABLES **4**
LIST OF FIGURES **5**
1 INTRODUCTION **6**
1.1 Security Target Identification 6
1.2 TOE Identification 6
1.3 Target of Evaluation (TOE) Overview 6
1.4 TOE Description 7
1.4.1 Architectural overview 7
1.4.2 Scope of Evaluation 10
1.4.3 Summary of security features 14
2 CC CONFORMANCE CLAIM **19**
3 TOE SECURITY PROBLEM DEFINITION **20**
3.1 Threats 20
3.2 Assumptions 20
4 SECURITY OBJECTIVES **22**
4.1 Security objectives for the TOE 22
4.2 Security Objectives for the Operational Environment 22
4.3 Security Objectives Rationale 23
5 EXTENDED COMPONENTS DEFINITION **24**
6 SECURITY REQUIREMENTS **25**
6.1 Conventions 25
6.2 Security Functional Requirements 25
6.2.1 Security Audit (FAU) 25
6.2.2 Cryptography 26
6.2.3 User Data Protection (FDP) 30
6.2.4 Identification and Authentication (FIA) 35
6.2.5 Security Management (FMT) 37
6.2.6 Protection of the TSF (FPT) 38
6.2.7 TOE access (FTA) 38
6.2.8 Trusted Path/Channels (FTP) 39
6.2.9 6.2.9 Resource utilization (FRU) 39

6.3 Security Functional Requirements Rationale 40
6.3.1 Security Requirements Dependency Rationale 40
6.3.2 Sufficiency and coverage 45
6.4 Security Assurance Requirements 46
6.5 Security Assurance Requirements Rationale 46
7 TOE SUMMARY SPECIFICATION 47
7.1 TOE Security Functional Specification 47
7.1.1 Authentication 47
7.1.2 Access Control 47
7.1.3 L2 Traffic Forwarding 48
7.1.4 L3 Traffic Forwarding 48
7.1.5 Auditing 49
7.1.6 Communication Security 50
7.1.7 ACL 51
7.1.8 Security Management 51
7.1.9 User Security 52
7.1.10 Denial-of-Service Protection 53
7.1.11 Cryptographic functions 54
7.1.12 Time 54
7.1.13 SNMP Trap 54
7.1.14 STP 54
8 ABBREVIATIONS, TERMINOLOGY AND REFERENCES 56
8.1 Abbreviations 56
8.2 Terminology 56
8.3 References 57

List of Tables

Table 1: TOE CloudEngine chassis Series Switch Component Specifications 12
Table 2: TOE CloudEngine Box Series Switch Component Specifications 12
Table 3 List of software and guidance 12
Table 4: Access Levels 15
Table 5: Threats 20
Table 6: TOE Assumption 21

Table 7: Security Objectives for the TOE 22
Table 8: Security Objectives for the Operational Environment..... 23
Table 9: Rationale for threats 23
Table 10: Rationale for assumptions 23
Table 11: Dependencies between TOE Security Functional Requirements..... 44
Table 13: Objectives to SFR mapping rationale 46

List of Figures

Figure 1: TOE Physical architecture of Chassis Switch 7
Figure 2: TOE Physical Architecture of Box Switch 8
Figure 3: TOE Software architecture 9
Figure 4: TOE logical scope 13

1 Introduction

This Security Target is for the evaluation of Huawei CloudEngine Series Switch V100R002.

1.1 Security Target Identification

Name:	Huawei CloudEngine Series Switch V100R002 Security Target
Version:	0.8
Publication Date:	2013-11-13
Author:	Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name:	Huawei CloudEngine Series Switches
Version:	V100R002
Build:	C00SPC200
Sponsor:	Huawei
Developer:	Huawei
Keywords:	Huawei, VRP, Versatile Routing Platform, Ethernet Switches

1.3 Target of Evaluation (TOE) Overview

The CloudEngine series switches are next-generation, high-performance core switches designed for data center networks and high-end campus networks. The CloudEngine series switches provide stable, reliable, secure, and high-performance L2/L3 switching capabilities, helping build a scalable, virtualized, and converged network.

At the core of each switch is the Versatile Routing Platform Version 8 Release 6 (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include different interfaces with according access levels for administrators; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

Huawei CloudEngine Series Switches are classified into Box Switches and Chassis Switches based on their physical forms. The forward capacity of Chassis Switches is larger than Box Switches and Chassis Switches can use different LPU (Line Processing Unit) to provide different ports with various types, but there is no difference in security functionality. CloudEngine 12800 series switches are chassis switches, CloudEngine 5800 and CloudEngine 6800 series switches are box switches. The TOE requires some non-TOE hardware/software, these could be found in section 1.4.2.2.

1.4 TOE Description

1.4.1 Architectural overview

This section will introduce the Huawei CloudEngine Series Switch V100R002 from a physical architectural view and a software architectural view.

1.4.2.1 Physical Architecture

1.4.2.1.1 Physical Architecture of Chassis Switch

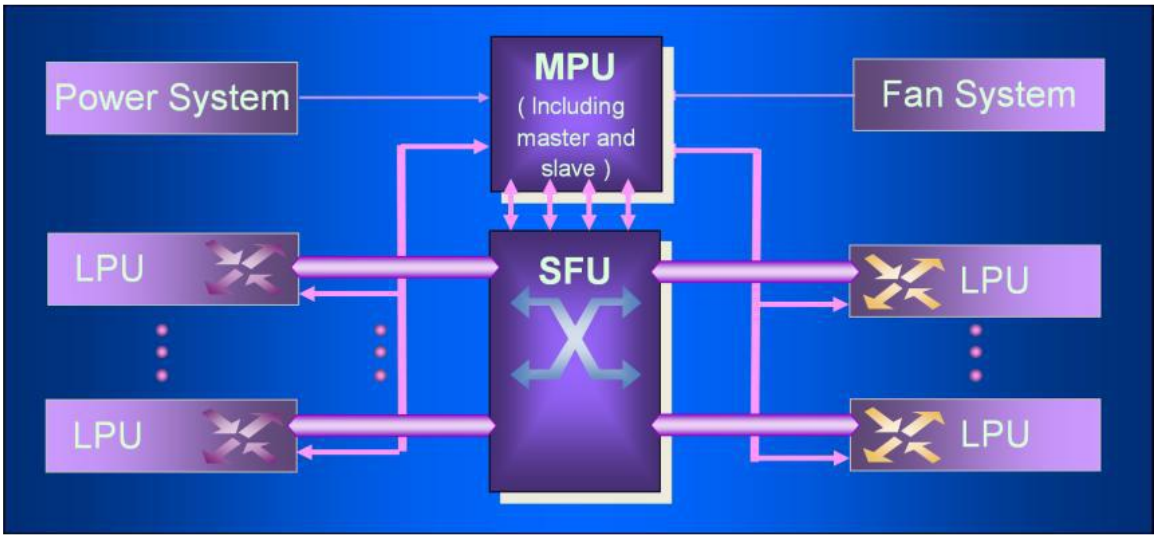

Figure 1: TOE Physical architecture of Chassis Switch

Figure 1 shows the physical architecture of Classis Switch with the AC/DC-input power supply modules. The physical architecture includes the following systems:

- Power system
- Fan system
- MPU (Main Processing Unit)
- SFU (Switch Fabric Unit)
- LPU (Line Process Unit)

All the systems are in the integrated cabinet. The power system works in 1+1 backup mode. The functional host system (MPU/SFU/LPU) is the main object of this evaluation and following introductions will focus on the functional host system only.

The functional host system is composed of the system backplane, MPU/LPU/SFU, SFU/MPU are the boards hosting the VRP which provides control and management functionalities. MPU also embeds a clock module as a source of system time. LPU is the board containing the forwarding engine and responsible for network traffic processing.

The functional host system processes data. In addition, it monitors and manages the entire system, including the power distribution system, heat dissipation system.

1.4.2.1.2 Physical Architecture of Box Switch

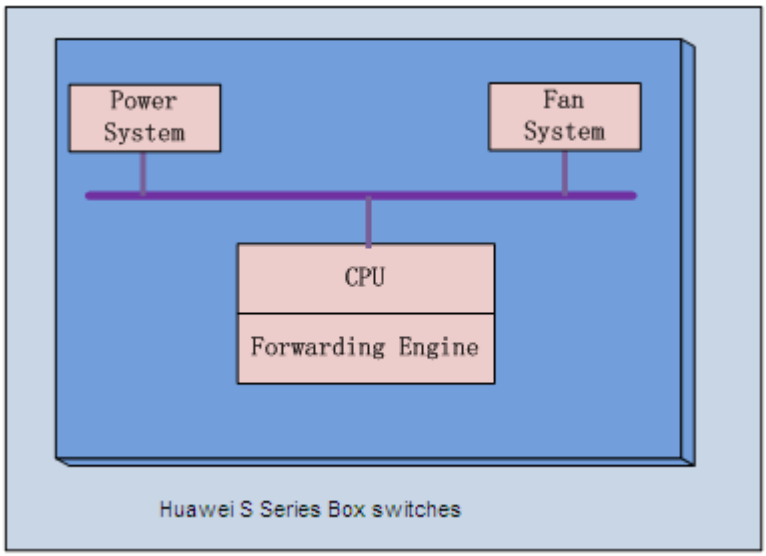

Figure 2: TOE Physical Architecture of Box Switch

Figure 2 shows the physical architecture of Box Switch of the TOE. The physical architecture includes the following systems:

- Power system
- Fan system
- CPU(Control Process Unit)
- Forwarding Engine

All systems are in the integrated cabinet. The power system works in 1+1 backup mode

1.4.2.2 Software Architecture

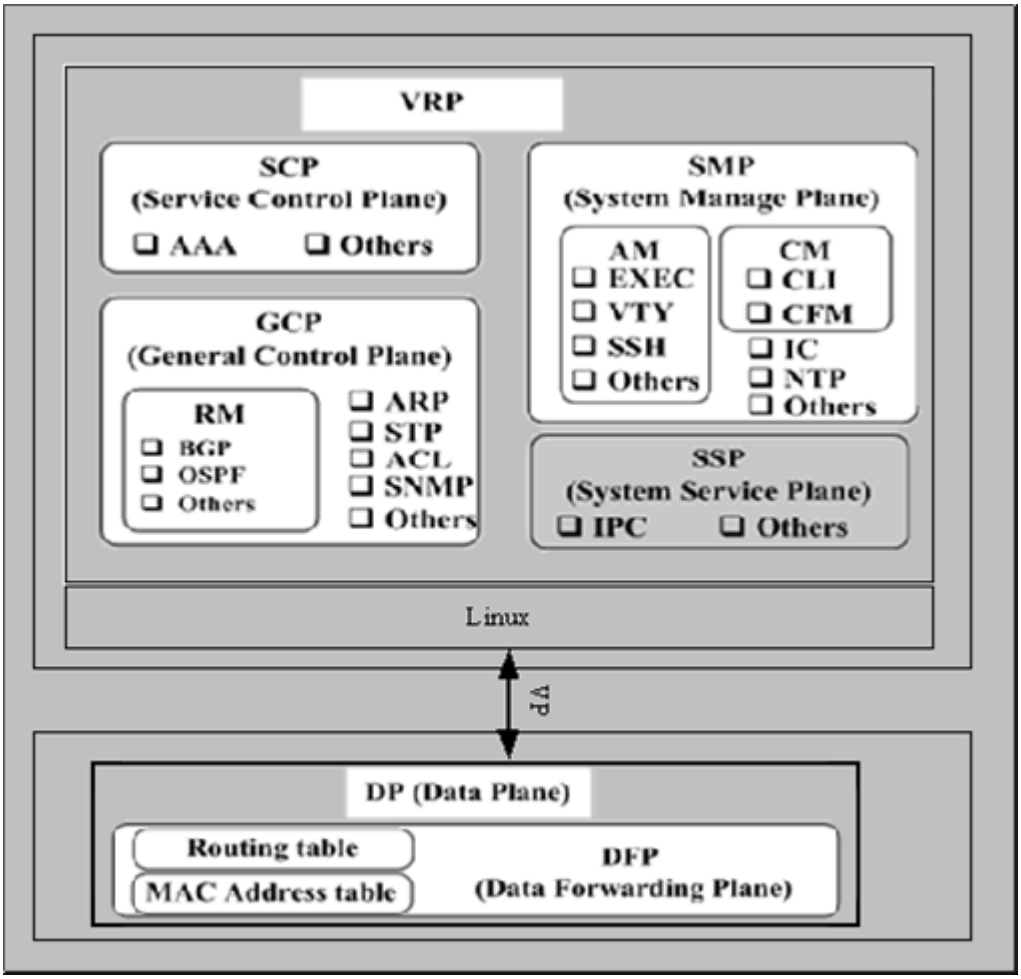

Figure 3: TOE Software architecture

For both box switches and Chassis switches, software architecture are same.

In terms of the software, the TOE's software architecture consists of three logical planes to support centralized forwarding and control and distributed forwarding mechanism.

- Data plane
- Control and management plane
- Monitoring plane

Note that the **monitoring plane** is to monitor the system environment by detecting the voltage, controlling power-on and power-off of the system, and monitoring the temperature and controlling the fan. The monitoring plane is not considered to be security-related.

The **control and management plane** is the core of the entire system. It controls and manages the system. The control and management unit processes protocols and signals, configures and maintains the system status, and reports and controls the system status.

The VRP is the control and management platform that runs on the SFU/MPU/LPU. The VRP supports IPv4/IPv6, and routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), calculates routes, generates forwarding tables, and delivers routing information to the LPU(s). The VRP includes Service Control Plane (SCP), System Management Plane (SMP), General Control Plane (GCP) and other TSF and non-TSF sub-systems.

The **data plane** is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, forwards IPv4/IPv6 packets, performs Quality of Service (QoS) and scheduling, completes inner high-speed switching, and collects statistics.

Figure 3 shows a brief illustration of the software architecture of the TOE.

1.4.2 Scope of Evaluation

This section will define the scope of the Huawei CE Series Switches V100R002 to be evaluated.

1.4.2.1 Physical scope

The physical boundary of the TOE is the actual switch system itself -- in particular, the functional host system. The power distribution system and heat dissipation system are part of the TOE but are security irrelevant.

The TOE provides several models. These models differ in their modularity and throughput but use the same version of software and have identical security functionality.

The following models will be covered during this evaluation:

Series name	Model name	Description
CloudEngine 12800 Series Switch   	Huawei CloudEngine 12800 Series 12-Slot Chassis (Also referred to as the 12812 Switch)	The Huawei CloudEngine 12800 Series 12812 support 12 LPU(Line Process Unit) . 12812 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 48 Tbit/s switching capacity. 12812 chassis support 2 MPU/6 SFU/2 CMU/12 LPU/12 PM/17 FAN.
	Huawei CloudEngine 12800 Series 8-Slot Chassis (Also referred to as the 12808 Switch)	The Huawei CloudEngine 12800 Series 12808 support 8 LPU(Line Process Unit) . 12808 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 32 Tbit/s switching capacity. 12808 Switch chassis support a maximum of 2 MPU/6 SFU/2 CMU/8 LPU/8 PM/13 FAN.
	Huawei CloudEngine 12800 Series 4-Slot Chassis (Also referred to as the 12804 Switch)	The Huawei CloudEngine 12800 Series 12804 support 4 LPU (Line Process Unit) . 12804 provides 2 Tbit/s per-slot bandwidth (can be increased to 4 Tbit/s) and a maximum of 16 Tbit/s switching capacity. 12804 Switch chassis support a maximum of 2 MPU/6 SFU/2 CMU/8 LPU/4 PM/9 FAN.
	Huawei CloudEngine 12800 Series Main Processing Unit MPUA (including master and	CE-MPUA is the main control unit of the CloudEngine 12800 series switches and is responsible for system control and management. The CE series switches can

	slave, plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	be configured with double CE-MPUAs to implement 1:1 hot backup. This configuration improves system reliability.
	Huawei CloudEngine 12800 Series Centralized Monitoring Unit CMUA (plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	The CE-CMUA is the Centralized Monitoring Unit of the CloudEngine 12800 series switches and provides highly reliable device monitoring, management, and energy saving functions. The CE series switches can be configured with double CE-CMUAs to implement 1:1 hot backup. This configuration improves system reliability.
	Huawei CloudEngine 12800 Series Switch Fabric Unit (plugs into either the 12-Slot or 8-Slot or 4-slot chassis)	The CE-SFUs are switch fabric units of the CE series switches that complete line-speed switching on the data plane. A maximum of six CE-SFUs can be installed in a chassis and work in load balancing and redundancy mode to improve system reliability.
	CE-L48GT-EA (48-Port 10/100/1000BASE-T Interface Card (EA, RJ45))	The CE-L48GT-EA provides forty-eight GE electrical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GS-EA (48-Port 100/1000BASE-X Interface Card (EA, SFP))	The CE-L48GS-EA provides forty-eight GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GT-EC (48-Port 10/100/1000BASE-T Interface Card (EC, RJ45))	The CE-L48GT-EC provides forty-eight GE electrical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48GS-EC (48-Port 100/1000BASE-X Interface Card (EC, SFP))	The CE-L48GS-EC provides forty-eight GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L24XS-BA (24-Port 10GBASE-X Interface Card (BA, SFP+))	The CE-L24XS-BA provides twenty-four 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L24XS-EA (24-Port 10GE Optical Interface Card (EA, SFP+))	The CE-L24XS-EA provides twenty-four 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48XS-BA (48-Port 10GBASE-X Interface Card (BA, SFP+))	The CE-L48XS-BA provides forty-eight 10GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.
	CE-L48XS-EA (48-Port 10GBASE-X Interface Card (EA, SFP+))	The CE-L48XS-EA provides forty-eight 10GE optical ports for data access and processing. which can be installed in any

		slot of the CE12804/12808/12812 chassis.
	CE-L24LQ-EA (24-Port 40G Interface Card (EA, QSFP+))	The CE-L24LQ-EA provides twenty-four 40GE optical ports for data access and processing. which can be installed in any slot of the CE12804/12808/12812 chassis.

Table 1: TOE CloudEngine chassis Series Switch Component Specifications

Series name	Model name	Description
CloudEngine 5800 Series Switch	CE5850-48T4S2Q-EI 	CE5850-48T4S2Q-EI: Provides forty-eight 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports, and two 40G QSFP+ Ethernet optical ports.
	CE5810-24T4S-EI 	CE5810-24T4S-EI：Provides twenty-four 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports.
	E5810-48T4S-EI 	CE5810-48T4S-EI：Provides forty-eight 10/100/1000BASE-T Ethernet ports, four 10G SFP+ Ethernet optical ports.
CloudEngine 6800 Series Switch	CE6850-48S4Q-EI 	CE6850-48S4Q-EI: Provides forty-eight 10G SFP+ Ethernet optical ports and four 40G QSFP+ Ethernet optical ports
	CE6850-48T4Q-EI 	CE6850-48T4Q-EI: Provides forty-eight 10G BASE-T Ethernet ports and four 40G QSFP+ Ethernet optical ports

Table 2: TOE CloudEngine Box Series Switch Component Specifications

The software and the guidance is listed in Table **3**

Type	Name	Version
Software	Product software	V100R002
	VRP	Version 8 Release 6
	Linux	Version: 2.6.34.12-WR4.3.0.0
Guidance	CloudEngine 6800&5800 Product Documentation	V1.0
	CloudEngine 12800 Product Documentation	V1.0
	CC Huawei CE Series Switches V100R002 - AGD_OPE	V1.0
	CC Huawei CE Series Switches V100R002 - AGD_PRE	V1.0

Table 3 List of software and guidance

1.4.2.2 Logical scope

The logical boundary is represented by the elements that are displayed with a white background within the rectangle with dashed border.

These elements are part of the Versatile Routing Platform (VRP), a software platform from view of software architecture, and the forwarding engine that processes the incoming and outgoing network traffic.

Figure 4 shows the TOE's logical scope with supporting network devices of the environment.

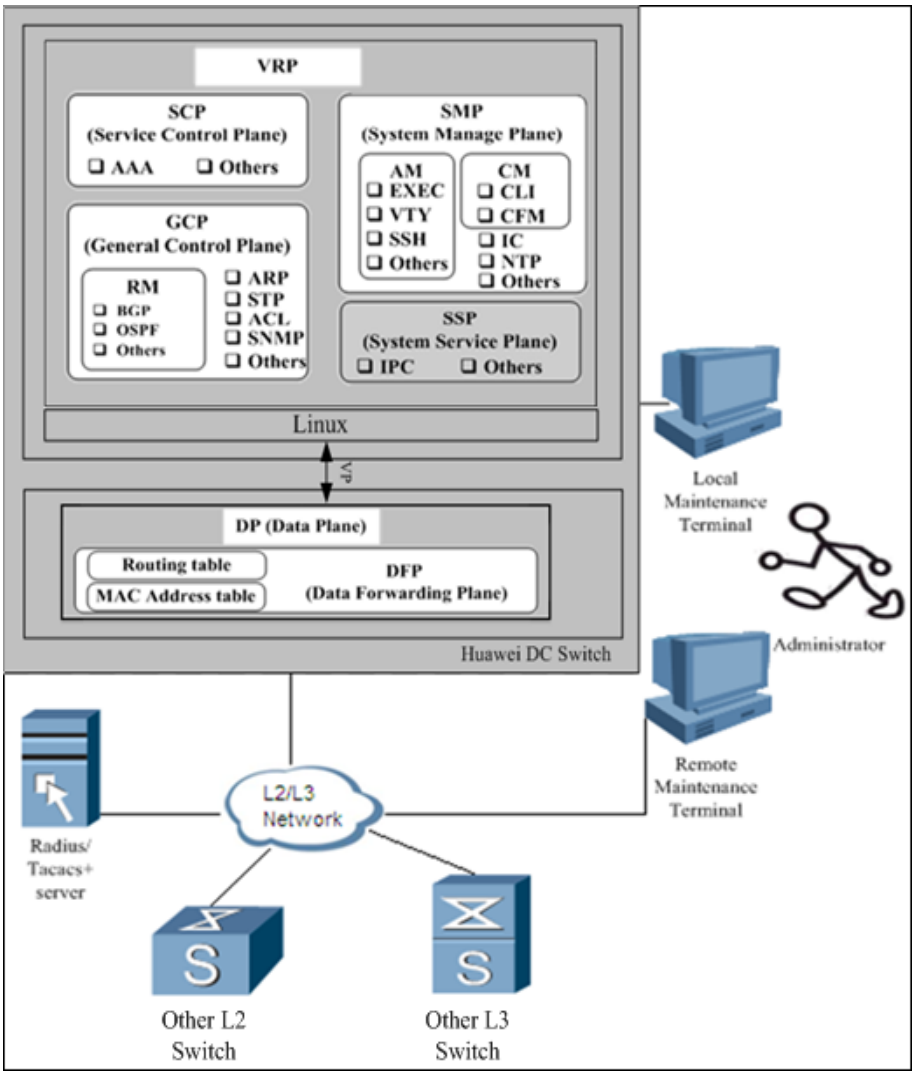

Figure 4: TOE logical scope

The TOE can operate as both a Layer 2 and a Layer 3 forwarding device. When operating as a Layer 2 forwarding device, the forwarding engine of TOE will forward the traffic according to MAC address. The MAC table entry will be automatically created by forwarding engine when Layer 2 forwarding.

When operating as a Layer 3 forwarding device，the TOE controls the flow of IP traffic between network interfaces by matching information contained in the headers of IP packets against routing table in forwarding engine. The routing table in forwarding engine is delivered from VRP's routing unit whereas the routing table in VRP's routing

module can be statically configured or imported through dynamic routing protocol such as BGP, Open Shortest Path First (OSPF).

System control and security managements are performed either through a local interface or through an interface protected by SSH.

Based on physical scope and logical scope described so far, a list of configuration is to be added:

- For management via the console, authentication is always enabled. When a user logs in for the first time, the TOE will prompt the user to configure password or no password. If the user chooses “no password”(not recommended) then the TOE will allow console login without authentication. Length of password is no less than 8 characters.
- For management via the ETH interface in MPU, authentication is always enabled. Authentication mode is password. Length of password is no less than 8 characters
- Service of TELNET and FTP are disabled in this evaluation.
- Authentication of users via RSA when using SSH connections is supported. SSH server compatibility with version number less than 1.99 is considered a weakness, therefore to be disabled.

The environment for TOE comprises the following components:

- An optional Radius or TACACS+ server providing authentication and authorization decisions to the TOE
- Other switches and routers used to connect the TOE for L2/L3 network forward, L3 switch providing routing information to the TOE via dynamic protocols, such as BGP, OSPF.
- Local PCs used by administrators to connect to the TOE for access of the command line interface either through TOE’s console interface or TOE’s ETH interface via a secure channel enforcing SSH.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on LPU within the TOE via a secure channel enforcing SSH.
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

1.4.3 Summary of security features

Authentication The TOE can authenticate administrative users by user name and password. VRP provides a local authentication scheme for this, or can optionally enforce authentication decisions obtained from a Radius or TACACS+ server in the IT environment. Authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP) sessions.

Access Control: The TOE access control is performed by VRP and includes the following:

- ✓ Users can be configured with different user levels to control their device access. User levels are configured by an administrator.
- ✓ User levels are marked by numbers from 0 to 15, where 0 is low privilege and 15 is full privilege
- ✓ User levels map to command levels (groups of commands). A user can run only commands at the same or lower level.

User level	Command level	Level name	Description
0	0	Visit	Commands at this level are diagnosis commands such as ping and trace commands and commands that are used to access a remote device such as Telnet clients.
1	0,1	Monitoring	Commands at this level are system maintenance commands such as most display commands.
2	0,1,2	Configuration	Commands at this level are used for service configuration including routing commands and commands at each network layer to provide network services to users.
3-15	0,1,2,3	Management	Commands at this level are system basic operation commands that support services, including file system, FTP, TFTP, configuration file switching commands, user management commands, command level configuration commands, system parameter configuration commands, and debugging commands.

Table 4: Access Levels

The TOE can either decide the authorization level of a user based on its local database, or make use of RADIUS or TACACS+ servers to obtain the decision whether a specific user is granted a specific level.

L2 Traffic Forwarding The TOE handles layer 2 forwarding policy at their core. The forwarding engine controls the flow of network packets by making (and enforcing) a decision with regard to the network interface that a packet gets forwarded to.

These decisions are made based on a MAC table. The MAC table is either maintained by administrators (static MAC) or gets updated dynamically by MAC learning function when a unknown MAC address packet has been received

L3 Traffic Forwarding The TOE handles forwarding policy at their core. The forwarding engine controls the flow of network packets by making (and enforcing) a decision with regard to the network interface that a packet gets forwarded to.

These decisions are made based on a routing table. The routing table is either maintained by administrators (static routing) or gets updated dynamically by the TOE when exchanging routing information with peer routers, through OSPF or BGP.

Auditing The TOE generates audit records for security-relevant management actions and stores the audit records in memory in the TOE.

- By default all correctly input and executed commands along with a timestamp when they are executed are logged.

- Authentication attempts are logged, regardless of success or failure, along with user ID, source IP address, timestamp etc.
- Administrators can select which events are being audited by enabling auditing for individual modules (enabling audit record generation for related to functional areas), and by selecting a severity level. Based on the hard-coded association of audit records with modules and severity levels, this allows control over the types of audit events being recorded.
- Output logs to various channels such as monitor, log buffer, trap buffer, file, etc.
- Review functionality is provided via the command line interface, which allows administrators to inspect the audit log.

Communication Security The TOE provides communication security by implementing SSH2.0 protocol:

- authentication by password, by RSA/DSA/ECC or by password with RSA/DSA/ECC;
- 3DES/AES encryption algorithms
- Secure cryptographic key exchange by DH-exchange-group, DH-group1
- MD5 is used as optional HMAC algorithm for SSH;
- HMAC-MD5/ SHA1/SHA2 is used as verification algorithm for packets of SSH protocols

Security functionality management This includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters, enabling/.disabling SSH, enabling and configuring BGP, OSPF, ARP, managing audit functionality etc.

User Security The TOE offers an Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces. The administrator can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against ACL rules specified. Source MAC address, Destination MAC address, Ethernet protocol type, Source IP address, destination IP address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, type and code if ICMP protocol, fragment flag etc., can be used for ACL rule configuration.

To prevent attackers bypassing this ACL (and other attacks), the TOE also offers:

- **Port security** which checks whether the source MAC addresses of data frames received on an interface are valid and takes action if they are not.
- **DHCP snooping**, which intercepts and analyzes DHCP messages transmitted between DHCP clients and a DHCP server, and, from these messages DHCP snooping creates and maintains a DHCP snooping binding table, which is used by IP Source Guard and Dynamic ARP Inspection (see further). DHCP snooping also filters out messages from/to unauthorized DHCP servers.
- **IP Source Guard**, which the TOE uses to check IP packets against the DHCP snooping binding table and thereby filters out packets that do not match this table (and therefore have probably forged their IP address).
- **Dynamic ARP inspection** (DAI) allows the device to compare the source IP address, source MAC address, interface number, and VLAN ID of an ARP packet with the DHCP snooping binding table. If an entry is matched, the device considers the ARP packet valid

and allows the packet to pass through. If no entry is matched, the device considers the ARP packet invalid and discards the packet.

Denial-of-Service Protection

The TOE uses two specific mechanisms to prevent Denial of Service against itself or the network it protects:

- **CPCAR** (Control Plane Committed Access Rate) limits the rate of protocol packets sent to the control plane and schedules the packets to protect the control plane. The switch identifies service packets based on ACLs and applies the default CAR value to protocol packets so that a limited number of protocol packets are sent to the control plane. Security of the control plane is ensured. CPCAR can be used to set the rate at which classes of packets are sent to the CPU, or the total rate of packets sent to the CPU. When the rate exceeds the upper limit, the system discards excess packets to prevent CPU overload
- **Traffic suppression** limits the number of unknown unicast packets, multicast packets, and broadcast packets within a proper range to ensure network efficiency. The TOE can suppress the packets based on interfaces and VLANs. When traffic suppression is enabled on an interface, the TOE checks whether the traffic volume of unknown unicast packets, multicast packets, and broadcast packets received by the interface monitors exceeds the threshold. If the traffic volume exceeds the threshold, the CloudEngine Series Switch discards excess packets to keep the traffic volume within the limit to ensure that services run properly.

Cryptographic functions

Cryptographic functions are required by security features as dependencies, where:

1) AES256 is used as default encryption algorithm for SSH;
2) 3DES and AES128 are used as optional encryption algorithm for SSH;
3) RSA/DSA/ECC or password used when user tries to authenticate and gain access to the TOE.
4) MD5 is used as option of HMAC algorithm for SSH packet verification;
5) MD5 is used as verification algorithm for packets of BGP and OSPF protocols from peer network devices;

SNMP Trap The Simple Network Management Protocol (SNMP) is a network management protocol widely used in the TCP/IP network. SNMP is a method of managing network elements through a network console workstation which runs network management software.

A trap is a type of message used to report an alert or important event about a managed device to the NM Station. The TOE uses SNMP traps to notify a fault occurs or the system does not operate properly.

The TOE provides SNMP v3 for secure channel between device and NMS. NMS can use v3 AES128 encryption technique with SHA Authentication.

STP (Spanning-Tree Protocol) is a protocol used in the local area network (LAN) to eliminate loops. The S-switch devices enabled with STP communicate and find the loops in the network, and they block certain interfaces to eliminate loops. Due to the rapid increase of LAN, STP has become one of the most important LAN protocols.

In the Layer 2 switching network, loops on the network cause packets to be continuously duplicated and propagated in the loops, leading to the broadcast storm, which exhausts all the available bandwidth resources and renders the network unavailable.

In an STP region, a loop-free tree is generated. Thus, broadcast storms are prevented and redundancy is implemented.

2 CC Conformance Claim

This ST is CC Part 2 conformant and CC Part 3 conformant. The CC version of [CC] is 3.1R4.

No conformance to a Protection Profile is claimed.

No conformance rationale to a Protection Profile is claimed.

The TOE claims EAL3+ augmented with ALC_CMC.4 (instead of ALC_CMC.3).

3 TOE Security problem definition

3.1 Threats

The **information assets** to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, audit records, etc.) and other information that the TOE facilitates access to (such as system software, patches and network traffic routed by the TOE) are all considered part of information assets.

Table 5 lists the threats addressed by the TOE and the IT Environment

Threat Name	Threat Definition
T.UnwantedTraffic	Unwanted traffic sent to/through the TOE will: - cause the TOE and/or resources on the network to become too slow or unavailable, or - reach resources on the network that it is not allowed to reach.
T.UnauthenticatedAccess	A user who is not an administrator gains access to the management interface of the TOE.
T.UnauthorizedAccess	An administrator authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
T.Eavesdrop	An eavesdropper (remote attacker) is able to intercept, and potentially modify or re-use information assets that are exchanged between: • TOE and LMT/RMT (management traffic) • TOE and the SNMP Trap Server (SNMP Traps) • TOE and other routers/switches (routing information)

Table 5: Threats

3.2 Assumptions

Table 6 lists the assumptions that are upheld for the operational environment of the TOE.

Assumption Name	Assumption Definition
A.PhysicalProtection	It is assumed that the TOE (including any console attached)is protected against unauthorized physical access.
A.NetworkElements	The environment is supposed to provide supporting mechanism to the TOE: • A Radius server or TACACS+ server for external authentication/authorization decisions; • Peer router(s) for the exchange of dynamic routing information;

	• Remote entities (PCs) used for administration of the TOE. • An SNMP Server used for collecting SNMP traps
A.NetworkSegregation	It is assumed that the ETH interface in the TOE will be accessed only through an independent local network This network is separate from the networks that use the other interfaces of the TOE.
A.NoEvil	The authorized administrators are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Table 6: TOE Assumption

4 Security Objectives

4.1 Security objectives for the TOE

TOE Security Obj.	Definition
O.DeviceAvail	The TOE shall ensure its own availability
O.UserAvail	The TOE shall ensure authorized users can access network resources through the TOE.
O.DataFilter	The TOE shall ensure that only allowed traffic goes through the TOE.
O.Communication	The TOE shall protect the network communication between: • the TOE and LMT/RMT (management information) • the TOE and the SNMP trap server (SNMP Traps) • the TOE and other switches/routers (routing information)
O.Authorization	The TOE shall allow different authorization levels to be assigned to administrators in order to restrict the functionality that is available to individual administrators.
O.Authentication	The TOE shall authenticate users before allowing them access to its management interface
O.Audit	The TOE shall generate audit records for security-relevant administrator actions.

Table 7: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

Environment Security Objective	Definition
OE.NetworkElements	The operational environment shall provide secure and correct working network devices as resources that the TOE needs to cooperate with, such as: (when required): • A Radius server or TACACS+ server for external authentication/authorization decisions; • Peer router(s) for the exchange of dynamic routing information; • Remote entities (PCs) used for administration of the TOE. • An SNMP Server used for collecting SNMP traps
OE.Physical	The operational environment shall protect the TOE against unauthorized physical access.

OE.NetworkSegregation	The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network This network is separate from the networks that use the other interfaces of the TOE.
OE.Person	Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE

Table 8: Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

Threat	Rationale for security objectives to remove threats
T.UnwantedTraffic	This threat is countered by O.DeviceAvail, ensuring the TOE remain available, O.UserAvail ensuring the network remains available and O.DataFilter ensuring that unwanted data is filtered and cannot access the network resources.
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSHv2 for communication between LMT/RMT and the TOE and SNMPv3 for communication between the TOE and the SNMP Trap Server. (O.Communication).

Table 9: Rationale for threats

Assumption	Rationale for security objectives
A.NetworkElements	Directly covered by OE.NetworkElements.
A.PhysicalProtection	Directly covered by OE.Physical.
A.NetworkSegregation	Directly covered by OE.NetworkSegregation.
A.NoEvil	Directly covered by OE.Person.

Table 10: Rationale for assumptions

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

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) **[The following auditable events:**

i. user activity

1. login, logout

2. operation requests

ii. User management

1. add, delete, modify

2. password change

3. operation authority change

4. online user query

5. session termination

iii. command level management

1. add, delete, modify

iv. authentication policy modification

v. system management

1. reset to factory settings

vi. log management

1. log policy modification]

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, **[interface (if applicable), workstation IP (if applicable), User ID (if applicable), and CLI command name (if applicable)]**

6.2.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[the users of user level 3 to 15]** with the capability to read **[all 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.

6.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[selection]** of audit data based on **[filename].**

6.2.1.5 FAU_STG.1 Protected audit trail storage

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

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

6.2.1.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **[delete the oldest files]** if the audit trail exceeds **[the size of the storage device]*.***

6.2.2 Cryptography

6.2.2.1 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified cryptographic algorithm **[AES CBC Mode]** and cryptographic key sizes **[128bits, 256bits]** that meet the following: **[FIPS 197]**

6.2.2.2 FCS_COP.1/3DES Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified cryptographic algorithm **[3DES Outer CBC Mode]** and cryptographic key sizes **[168bits]** that meet the following: **[FIPS PUB46-3]**

6.2.2.3 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric authentication]** in accordance with a specified cryptographic algorithm **[RSASSA-PKCS-v1_5 with SHA1]** and cryptographic key sizes **[configured (512bits-2048bits)]** that meet the following: **[RSA Cryptography Standard (PKCS#1)]**

6.2.2.4 FCS_COP.1/MD5 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **authentication** in accordance with **a specified cryptographic algorithm MD5** and cryptographic key sizes **none** that meet the following: **RFC 1321**

6.2.2.5 FCS_COP.1/HMAC-MD5 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[authentication]** in accordance with a specified cryptographic algorithm **[HMAC-MD5]** and cryptographic key sizes **[16 bytes]** that meet the following: **[RFC 2104]**

6.2.2.6 FCS_COP.1/DHKeyExchange Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[Diffie-Hellman key agreement]** in accordance with a specified cryptographic algorithm **[diffie-hellman-group1-sha1 and diffie-hellman-group-exchange-sha1]** and cryptographic key sizes **[diffie-hellman-group1-sha1: 1024 bits Oakley Group 2, diffie-hellman-group-exchange-sha1: 1024bits to 8192bits]** that meet the following: [**RFC 4253/RFC4419]**

6.2.2.7 FCS_COP.1/ECC Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric authentication]** in accordance with a specified cryptographic algorithm **[ECDSA]** and cryptographic key sizes **[configured (256, 384, 521 bits)]** that meet the following: **[ECC Cryptography Standard (RFC5656, SEC-2 standard)]**

6.2.2.8 FCS_COP.1/DSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[asymmetric authentication]** in accordance with a specified cryptographic algorithm **[DSA]** and cryptographic key sizes **[configured (512, 1024 & 2048bits)]** that meet the following: **[DSA Cryptography Standard (FIPS-186-3)]**

6.2.2.9 FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSH key derivation]** and specified cryptographic key sizes **[128bits, 256bits]** that meet the following:**[RFC 4253]**

6.2.2.10 FCS_CKM.1/3DES Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSH key derivation]** and specified cryptographic key sizes [**168bits]** that meet the following: **[RFC 4253]**

6.2.2.11 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA]** and specified cryptographic key sizes **[configured (512bits-2048bits)]** that meet the following: **[RSA Cryptography Standard (PKCS#1)]**

6.2.2.12 FCS_CKM.1/HMAC_MD5 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSH key derivation]** and specified cryptographic key sizes **[16 bytes]** that meet the following:**[RFC 4253]**

6.2.2.13 FCS_CKM.1/DHKey Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[DH Group Generation]** and specified cryptographic key sizes **[1024bits to 8192 bits]** that meet the following: **[RFC4419]**

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSH key derivation]** and specified cryptographic key sizes **[16 bytes]** that meet the following: **[RFC 4253]**

6.2.2.14 FCS_CKM.1/ECC Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[EC-DSA keygen method]** and specified cryptographic key sizes **[configured (256, 384 and 521bits)]** that meet the following: **[ECC Cryptography Standard (RFC5656, SEC-2 standard)]**

6.2.2.15 FCS_CKM.1/DSA Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[DSA]** and specified cryptographic key sizes **[configured (512, 1024 & 2048bits)]** that meet the following: **[DSA Cryptography Standard (FIPS-186-3)]**

6.2.2.16 FCS_CKM.4/3DES-AES Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[releasing memory so that it is eventually overwritten]** that meets the following: **[none]**

6.2.2.17 FCS_CKM.4/RSA Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwriting with 0]** that meets the following: **[none]**

6.2.2.18 FCS_CKM.4/HMAC_MD5 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy HMAC_MD5 keys in accordance with a specified cryptographic key destruction method **[Releasing Memory]** that meets the following: **[none]**

6.2.2.19 FCS_CKM.4/DHKey Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[Releasing Memory]** that meets the following: **[none]**

6.2.2.20 FCS_CKM.4/ECC Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwriting with 0]** that meets the following: **[none]**

6.2.2.21 FCS_CKM.4/DSA Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwriting with 0]** that meets the following: **[none]**

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[VRP access control policy]** on

[Subject: users;

Objects: commands /features provided by TOE;

Operation: Read access / write access /Deny access]

6.2.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[VRP access control policy]** to objects based on the following:

[Subject security attributes

a) users and their following security attributes:

- **user Identity**
- **user level assignment**

Objects security attributes:

a) commands and their following security attributes:

- **Commands and command level]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among

controlled subjects and controlled objects is allowed: **[**

a) Only authorized users are permitted access to commands and feature.

b) Users can be configured with different user levels to control the device access permission.

c) There are 16 user levels numbered from 0 to 15, in ascending order of priorities.

d) User levels map command levels. A user can only run commands at the same or lower level.

Above mentioned information is identified in table 4.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[**

a) the user has been granted authorization for the relevant level commands]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[**

a) the user has not been granted authorization for the commands targeted by the request, or

b) the user is not granted authorization with a Command beyond user relevant level].

6.2.3.3 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **[the authentication information of BGP, OSPF, SSH, SNMP]**

FDP_DAU.1.2 The TSF shall provide **[BGP, OSPF, SSH, SNMP]** with the ability to verify evidence of the validity of the indicated information.

6.2.3.4 FDP_IFC.1(1) Subset information flow control- CPU-defend

FDP_IFC.1.1(1) The TSF shall enforce **[Control Plane Committed Access Rate (CPCAR)/Blacklist]** on

[Subjects:

TOE interface through which traffic goes

Information:

Ingress Control Plane Traffic (all different types of packets can reach the control plane, such as routing protocol or exception packets (ip options .etc), control traffic);

Operations:

Transmit Control Plane Traffic Flow;

Drop Control Plane Traffic Flow;

CAR(QoS) the Control Plane Traffic Flow;]

6.2.3.5 FDP_IFC.1(2) Subset information flow control- Data plane traffic control

FDP_IFC.1.1(1) The TSF shall enforce **[ACLs]** on

[Subjects:

TOE interface through which traffic goes

Information:

Traffic flows;

Operations:

Permit, Deny, CAR]

6.2.3.6 FDP_IFF.1(1) Simple security attributes - CPU-defend

FDP_IFF.1.1(1) The TSF shall enforce the **[Control Plane Committed Access Rate (CPCAR)/Blacklist]** based on the following types of subject and information security attributes**[**

Subject: TOE logic CPU- interface through which traffic goes.

Subject security attributes:

- ✓ **Configured Rate Limit per traffic type**
- ✓ **Packets per second permitted to control plane**
- ✓ **filtering traffic destined to CPU by blacklist**

Information security attributes:

- ✓ **Receive packets: Packets destined to device. such as OSPF/LLDP/STP/VRRP.etc**
- ✓ **Snooping packets: Packets which is monitored. Such as DHCP Snooping and ARP inspection packets**
- ✓ **Packets which need further process: such as ARP miss packets, unknown multicast .etc**

- ✓ **filtering traffic destined to CPU by blacklist**

]

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

- ✓ **If the ingress Control Plane Traffic with security attributes that match the configured Control Plane packets type (OSPF/LLDP .etc.) does not exceed the configured rate limits, the traffic is permitted to flow**
- ✓ **If the ingress Control Plane Traffic with security attributes that match the configured Control Plane packets type (OSPF/LLDP .etc.) exceed the configured rate limits, the traffic is not permitted to flow and will be dropped.]**

FDP_IFF.1.3(1) The TSF shall enforce the **[traffic statistic]**.

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: **[none]**

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:**[none]**

6.2.3.7 FDP_IFF.1(2) Simple security attributes – Data plane traffic control

FDP_IFF.1.1(2) The TSF shall enforce the **[ACLs]** based on the following types of subject and information security attributes **[**

Subject: TOE interface through which traffic goes

Subject security attributes:

Port security / IPSG /DHCP Snooping –DAI

Information security attributes:

Packet characteristic: such as Source MAC address /Destination MAC address / Source IP address / Destination IP address / protocol type /Source port / Destination port /VLAN value /COS/DSCP value .etc.]

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Network traffic is match TOE according to administratively configured policies

The specific information flow control rules associated with each policy are as follows:

ACL

Ingress or egress IP traffic with security attributes that match configured ACL policy rule will be processed according to that rule.

Port security

Port security is a security mechanism that controls network access. This mechanism checks whether the source MAC addresses of data frames received on an interface are valid. When detecting packets with invalid source MAC addresses, the mechanism takes actions to protect the interface. The TOE considers the following types of MAC addresses valid:

- ✓ Static MAC addresses that are manually configured
- ✓ Secure dynamic MAC addresses
- ✓ Sticky MAC addresses
- ✓ When an interface receives frames with invalid source MAC addresses, the TOE discards the frames or generates an alarm accordingly.

IPSG

- ✓ IPSG enables the device to check IP packets against dynamic and static DHCP entries.
- ✓ Before the device forwards an IP packet, it compares the source IP address, source MAC address, interface, and VLAN information in the IP packet with entries in the binding table. If an entry is matched, the device takes the IP packet as a valid packet and forwards an IP packet.

Otherwise, the device takes the IP packet as an attack packet and discards the packet.

DHCP Snooping – DAI

DHCP snooping intercepts and analyzes DHCP messages transmitted between DHCP clients and a DHCP server. DHCP snooping creates and maintains a DHCP snooping binding table, and filters untrusted DHCP messages according to the table. The binding table contains the MAC address, IP address, lease, binding type, VLAN ID, and interface number.

DHCP snooping ensures that authorized users can access the network by recording the mapping between IP addresses and MAC addresses of clients. In this manner, DHCP snooping could acts as a firewall between DHCP clients and a DHCP server.

Dynamic ARP inspection (DAI) allows the device to compare the source IP address, source MAC address, interface number, and VLAN ID of an ARP packet with a binding entry. If an entry is matched, the device considers the ARP packet valid and allows the packet to pass through. If no entry is matched, the device considers the ARP packet invalid and discards the packet.

Storm suppression

Traffic suppression limits the number of unknown unicast packets, multicast packets, and broadcast packets within a proper range to ensure network efficiency.

TOE checks whether the traffic volume of unknown unicast packets, multicast packets, and broadcast packets received by the interface monitors exceeds the threshold.

- ✓ If the traffic volume does not exceeds the threshold, packet is permitted to flow

If the traffic volume exceeds the threshold, the TOE discards excess packets to keep the traffic volume within the limit to ensure that services run properly**]**

FDP_IFF.1.3(2) The TSF shall enforce the **[none].**

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: **[DHCP packets from interfaces configured as trusted is permit to flow]**

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

- ✓ **For IPSG/DHCP snooping- DAI feature, packets that don’t match binding entry are dropped.**
- ✓ **For ACL feature, packets that match configured ACL with action “deny” are dropped**
- ✓ **For storm suppression feature, when traffic volume exceeds the threshold, are dropped.]**

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***[3]*** unsuccessful authentication attempts occur (since the last successful authentication of the indicated user identity) related to **[user logging in]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met]*****,** the TSF shall **[terminate the session of the authentication user]**.

6.2.4.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

a) user ID

b) user level

c) password]

6.2.4.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1/a The TSF shall provide a mechanism to verify that secrets meet **[for text string used as seeds for MD5 authentication for OSPF, they are case sensitive and contain no whitespace, no question mark. A cipher text mode should be used and the length of text string should be 32 to 392 characters]**

FIA_SOS.1.1/b The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for MD5 authentication for BGP, they are case sensitive and contain no whitespace, no question mark. A cipher password mode should be used and the length of password should be 32 to 392 characters]**

FIA_SOS.1.1/c The TSF shall provide a mechanism to verify that secrets meet **[for password used as seeds for user authentication for SSH and they are case sensitive. A cipher password mode should be used and the length of password should be at least 8 characters long]**

Application Note: All passwords must contain at least two normal characters, two capitals, 2 numbers and 2 special characters**.**

6.2.4.3 FIA_UAU.1 Timing of authentication –Administrator Authentication

FIA_UAU.1.1 The TSF shall allow **[establishment of a secure remote session between the administrative user and the TOE component]** 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.

6.2.4.6 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **[the following authentication mechanisms:**

a) Remote authentication (by RADIUS or TACACS+);

b) Local Authentication by local database local of TOE]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's identity according to the following: **[**

a) For Remote authentication by RADIUS or TACACS+

b) For local Authentication, the TSF will authenticate the administrator based on the configured Identification and Authentication scheme].

6.2.4.7 FIA_UID.1 Timing of identification – Administrator Identification

FIA_UID.1.1 The TSF shall allow **[establishment of a secure remote session between the administrative user and TOE component]** 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.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***[determine the behavior of]*** all the functions **[defined in FMT_SMF.1]** to **[the administrator-defined roles]**.

6.2.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/1 The TSF shall enforce the **[VRP access control policy]** to restrict the ability to ***[query, modify]*** the security attributes **[identified in FDP_ACF.1 and FIA_ATD.1]** to the **[administrator-defined roles]**.

FMT_MSA.1.1/2 The TSF shall enforce the **[VRP information control policy (based on ACL)]** to restrict the ability *to* ***[query, modify, delete]*** the security attributes **[identified in FDP_IFF.1]** to **[the roles which can match the VRP information control policy (based on ACL) and the policy action is permit]**.

6.2.5.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1/1 The TSF shall enforce the **[VRP access control policy]** to provide ***[restrictive]*** default values for security attributes (Command Group associations) that are used to enforce the SFP.

FMT_MSA.3.1/2 The TSF shall enforce the **[VRP information control policy (based on ACL)]** to provide ***[restrictive]*** default values for security attributes that are used to enforce the SFP.

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

6.2.5.4 FMT_SMF.1 Specification of Management Functions

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

- **a) authentication, authorization, encryption[1] policy**
- **b) ACL policy**
- **c) user management**
- **d) definition of Managed Object Groups and Command Groups**
- **e) ipsg / port security / dhcp snooping –DAI / cpcar]**

6.2.5.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[administrator-defined roles]** (refer to table 4)**.**

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.6.2 FPT_FLS.1 Fail secure

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

packets to enter in an infinite switching loop .

6.2.7 TOE access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

[1] The encryption policy dictates which cryptographic algorithm / key length is used in which situation

FTA_SSL.3.1 The TSF shall terminate an interactive session after **[a time interval of user inactivity which can be configured.**

SSH session will be terminated after a period which can be configured]

6.2.7.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[**

- **a) authentication failure**
- **b) Source IP address doesn't match IP address configured in ACL for user management.]**

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***[remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[modification, disclosure]***.

FTP_TRP.1.2 The TSF shall permit ***[remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[remote management]***.

6.2.8.2 FTP_ITC.1 Trusted channel

FTP_ITC.1.1 The TSF shall provide a communication path between itself and (SNMP Trap Server) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted path for **[sending SNMP traps]**.

6.2.9 6.2.9 Resource utilization (FRU)

6.2.9.1 FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority (used as configured bandwidth) to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to **[controlled resources]** (bandwidth) shall be mediated on the basis of the subjects assigned priority.

6.2.9.2 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resource: **[bandwidth,**

MAC address table entries] that ***[subjects]*** can use ***[simultaneously]***

6.2.9.3 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of **[Spanning Tree Protocol (STP) to cut off the loops]** when the following failures occur**: [packets to enter in an infinite loop]**

6.3 Security Functional Requirements Rationale

6.3.1 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/AES Cryptographic key generation FCS_CKM.4/3DES-AES Cryptographic key destruction
FCS_COP.1/3DES Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or	FCS_CKM.1/3DES Cryptographic key generation

	FCS_CKM.1] FCS_CKM.4	FCS_CKM.4/3DES-AES Cryptographic key destruction
FCS_COP.1/RSA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA Cryptographic key generation FCS_CKM.4/RSA Cryptographic key destruction
FCS_COP.1/HMAC-MD5 Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/HMAC_MD5 Cryptographic key generation FCS_CKM.4/HMAC_MD5 Cryptographic key destruction
FCS_COP.1/DHKeyExchange Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DHKey Cryptographic key generation FCS_CKM.4//DHKey Cryptographic key destruction
FCS_COP.1/ECC Cryptographic operation FCS_CKM.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/ECC Cryptographic key generation FCS_CKM.4/ECC Cryptographic key destruction
FCS_COP.1/DSA Cryptographic operation	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DSA Cryptographic key generation FCS_CKM.4/DSA Cryptographic key destruction
FCS_CKM.1/AES Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/AES Cryptographic operation FCS_CKM.4/3DES-AES Cryptographic key destruction
FCS_CKM.1/3DES Cryptographic key generationFCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4FCS_COP.1	FCS_COP.1/3DES Cryptographic operation FCS_CKM.4/3DES-AES Cryptographic key destruction FCS_COP.1

FCS_CKM.1/RSA Cryptographic key generationFCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4FCS_CKM .4	FCS_COP.1/RSA Cryptographic operationFCS_CKM.4 FCS_CKM.4/RSA Cryptographic key destruction
FCS_CKM.1/DHKey Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DHKeyExchange Cryptographic operation FCS_CKM.4/DHKey Cryptographic key destruction
FCS_CKM.1/HMAC_MD5 Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/HMAC-MD5 Cryptographic operation FCS_CKM.4/HMAC_MD5 Cryptographic key destruction
FCS_CKM.1/DSA Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DSA Cryptographic operation FCS_CKM.4/DSA Cryptographic key destruction
FCS_CKM.1/ECC Cryptographic key generation	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/ECC Cryptographic operation FCS_CKM.4/ECC Cryptographic key destruction
FCS_CKM.4/RSA Cryptographic key destruction	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA Cryptographic key generation
FCS_CKM.4/3DES-AES Cryptographic key destruction FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/3DES Cryptographic key generation FCS_CKM.1/AES Cryptographic key generation
FCS_CKM.4/ECC Cryptographic key destructionFCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/ECC Cryptographic key generation
FCS_CKM.4/DHKey Cryptographic key destruction	[FDP_ITC.1, or FDP_ITC.2, or	FCS_CKM.1/DHKey Cryptographic key generation

	FCS_CKM.1]	
FCS_CKM.4/HMAC_MD5 Cryptographic key destruction	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/HMAC_MD5 Cryptographic key generation
FCS_CKM.4/DSA Cryptographic key destruction	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/DSA Cryptographic key generation
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_DAU.1	No Dependencies	None
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No Dependencies	None
FIA_SOS.1	No Dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	No Dependencies	None
FIA_UID.1	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FDP_IFC.1(1) FDP_IFC.1(2) FMT_SMR.1 FMT_SMF.1

FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTP_STM.1	No Dependencies	None
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None
FTP_ITC.1	No Dependencies	None
FPT_FLS.1	No Dependencies	None
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FRU_PRS.1	No Dependencies	None
FRU_RSA.1	No Dependencies	None

Table 11: Dependencies between TOE Security Functional Requirements

6.3.2 Sufficiency and coverage

Objective	SFRs	Rationale
O.DeviceAvail O.UserAvail	FDP_IFC.1(1) FDP_IFF.1(1)	These SFRs apply CPCAR and Blacklist features to process packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.
	FDP_IFC.1(2) FDP_IFF.1(2)	These SFRs apply IP Source Guard/DHCP Snooping-DAI Port Security and Storm Suppression features to make device available when facing attacks. These SFRs also apply ACL to limit both packets going to the Control/Management Plane and through the TOE further ensuring availability of TOE and network resources.
	FRU_PRS.1 FRU_RSA.1	These SFRS apply L2 traffic forwarding **.** The TOE forwards network traffic, enforcing decisions about the correct forwarding interface and assembling the outgoing network packets using correct MAC addresses
	FRU_FLT.1 FPT_FLS.1	These SFRS apply STP to cut off the potential loops on the network and provide Link redundancy
O.Communication	FTP_TRP.1	This SFR provides the secure communication between users and management interface of the TOE
	FTP_ITC.1	This SFR provides the secure communication between TOE and SNMP Trap Server
	FDP_DAU.1 FIA_SOS.1	These SFRs provide the secure communication between TOE and other switches/routers and ensure that the secrets for this are long enough.
	FCS_COP.1/* FCS_CKM.1/* FCS_CKM.4/*	These SFRS provide the cryptographic services for the secure communication above.
O.DataFilter	FDP_IFC.1(2) FDP_IFF.1(2)	These SFRs apply ACL to limit both packets going to the Control/Management Plane and through the TOE and thereby ensure that only protected traffic goes through.
O.Authentication	FIA_UID.1	These SFRs ensure that a user must identify and authenticate himself, either by local password or

	FIA_UAU.1 FIA_UAU.5	through RADIUS/TACACS servers.
	FTA_TSE.1 FIA_AFL.1 FTA_SSL.3	The SFRs support authentication by: • Refusing logins from certain IP addresses • Not allowing unlimited login attempts • Logging out users after an inactivity period • Ensuring password quality
O.Authorisation	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized admins can access certain functions
	FMT_SMR.1 FIA_ATD.1	These SFRs defines authorization levels and ensure that upon login an administrator gets the proper authorization level.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization level.
	FMT_MSA.1 FMT_MSA.3	These SFRs ensure that new admins only get limited access rights and specifies who can modify these access rights.
O.Audit	FAU_GEN.1, FAU_GEN.2 FPT_STM.1	These SFRs ensure that audit records can be generated of significant events and that these contain useful information, including the correct time of the events.
	FAU_SAR.1, FAU_SAR.3	These SFRs ensure that the correct users can read the correct information from the audit records.
	FAU_STG.1, FAU_STG.3	These SFRs ensure the audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.

Table 12: Objectives to SFR mapping rationale

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components augmented with ALC_CMC.4 (instead of ALC_CMC.3), as specified in [CC] Part 3. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 3 augmented with ALC_CMC.4 (instead of ALC_CMC.3), has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functional Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

7.1.1 Authentication

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. Detailed functions include:

1) Support authentication via local password. This function is achieved by comparing user information input with pre-defined user information stored in memory.
2) Support authentication via remote RADIUS/TACAS+ authentication server. This function is achieved by performing pass/fail action based on result from remote authentication server.
3) Support authenticate user login using SSH, by password authentication, ECC、DSA、RSA authentication, or combination. This function is achieved by performing authentication for SSH user based on method mentioned in 1).
4) Support logout when no operation is performed on the user session within a given interval. This function is achieved by performing count-down through timing related to clock function.
5) Support max attempts due to authentication failure within certain period of time. This function is achieved by providing counts on authentication failure.
6) Support limiting access by IP address. This function is achieved by comparing IP address of requesting session with configured value stored in memory.
7) Support for user individual attributes in order to achieve all the enumerated features: user ID, user level, and password.

(FCS_COP.1/RSA, FCS_COP.1/ECC, FCS_COP.1/DSA, FDP_DAU.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1, FTA_SSL.3, FTA_TSE.1, FTP_TRP.1)

7.1.2 Access Control

The TOE enforces an access control by supporting following functionalities:

1) Support 16 access levels. This function is achieved by storing number as level

in memory.

2) Support assigning access level to commands. This function is achieved by associating access level number with commands registered.
3) Support assigning access level to user ID. This function is achieved by associating access level number with user ID.
4) Support limiting executing commands of which the access level is less or equal to the level of user. This function is achieved by performing an evaluation that level of commands is less or equal to level of user. This limitation of access also prevents users from accessing or deleting log files if they have insufficient rights.

(FDP_ACC.1, FIA_ATD.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1)

7.1.3 L2 Traffic Forwarding

The TOE forwards network traffic, enforcing decisions about the correct forwarding interface and assembling the outgoing network packets using correct MAC addresses:

1) Support traffic isolation with VLANs
2) Support MAC address learning automatically
3) Support Layer 2 traffic forwarding based on MAC table entry
4) Support to configure MAC address statically
5) Support to configure black hole MAC address statically
6) Support to limit the learning number of MAC address
7) Support to convert the MAC address learnt dynamically to static MAC address
8) Support MAC address flapping protection
9) In order to configure all the enumerated settings the user must be an authenticated user with administrator-defined role.

(FDP_IFC.1(2), FDP_IFF.1(2), FRU_PRS.1, FRU_RSA.1)

7.1.4 L3 Traffic Forwarding

The TOE forwards network traffic, enforcing decisions about the correct forwarding interface and assembling the outgoing network packets using correct MAC addresses:

1) Support ARP/BGP/OSPF protocol. This function is achieved by providing implementation of ARP/BGP/OSPF protocol.

2) Support routing information generation via OSPF protocol. This function is provided by implementation of OSPF protocol.
3) Support routing information generation via BGP protocol. This function is provided by implementation of BGP protocol.
4) Support routing information generation via manual configuration. This function is achieved by storing static routes in memory.
5) Support importing BGP/static routing information for OSPF. This function is provided by implementation of OSPF protocol.
6) Support importing OSPF/static routing information for BGP. This function is provided by implementation of BGP protocol.
7) BGP support cryptographic algorithm MD5. This function is achieved by performing verification for incoming BGP packets using MD5 algorithm.
8) OSPF support cryptographic algorithm MD5. This function is achieved by performing verification for incoming OSPF packets using MD5 algorithm.
9) Support disconnection session with neighbor network devices. This function is achieved by locating and cleaning session information.
10) OSPF support routing information aggregation. This function is achieved by manipulating routes stored in memory.
11) OSPF support routing information filtering. This function is achieved by manipulating routes stored in memory.
12) Support ARP strict learning. This function is achieved by regulating ARP feature to accept entry generated by own ARP requests.
13) Support IPv4 traffic forwarding via physical interface. This function is achieved by making routing decision based on routes generated by BGP/OSPF/static configuration.
14) Support sending network traffic to VRP for central process where destination IP address is one of the interfaces' IP addresses of the TOE. This is achieved by checking whether the traffic's destination IP address is within the configured interfaces' IP addresses in the TOE. If it is, the traffic will be sent to VRP in MPU for central process.

(FCS_COP.1/MD5, FDP_IFC.1(2), FDP_IFF.1(2), FIA_SOS.1, FDP_DAU.1)

7.1.5 Auditing

The TOE can provide auditing ability by receiving all types of logs and processing them according to user's configuration:

1) Support classification based on severity level. This function is achieved where logging messages are encoded with severity level and output to log buffer.
2) Support enabling, disabling log output. This function is achieved by interpreting

enable/disable commands and storing results in memory. Log output is performed based on this result.

3) Support redirecting logs to various output channels: monitor, log buffer, trap buffer, log file. This function is achieved by interpreting commands and storing results in memory or in log files in CF card. Log channel for output is selected prior to execution of redirecting.
4) Support log output screening, based on filename. This function is performed by providing filtering on output.
5) Support querying log buffer. This function is achieved by performing querying operation with conditions input.
6) Support cleaning log buffer. This function is achieved by cleaning log buffer in memory.
7) Support to automatically remove oldest log files if audit files exceed the size of store device.

(FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.3)

7.1.6 Communication Security

The TOE provides communication security by implementing SSH protocol. Two versions of SSH: SSHv1 (SSH1.5) and SSHv2 (SSH2.0) are implemented. But SSH2 is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance. SFTP provide secure file transfer functionality.

1) Support SSHv1 and SSHv2. This function is achieved by providing implementation of SSHv1 and SSHv2.
2) Support diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1& SM2 as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1 and SM2 algorithm.
3) Support 3DES, AES encryption algorithm. This function is achieved by providing implementation of 3DES, AES algorithm.
4) Support HMAC-MD5 verification algorithm. This function is achieved by providing implementation of HMAC-MD5 algorithm.
5) Support using different encryption algorithm for client-to-server encryption and server-to-client encryption. This function is achieved by interpreting related commands and storing the result in memory.
6) Support Secure-FTP. This function is achieved by providing implementation of Secure-FTP.
7) Support for RSA/DSA/ECC key construction and destruction by overwriting it

with 0.

(FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4/*, FMT_SMF.1, FDP_DAU.1)

7.1.7 ACL

TOE use ACL to deny unwanted network traffic to pass through itself.

ETH-based ACL is provided for this situation to identify traffic flow by matching all or part of vlan, mac destination address, mac source address, L2 protocol number etc, then to proceed with certain actions like rate limit, prioritization or discard.

IP-based ACL is provided for this situation to identify traffic flow by matching all or part of IP source address, IP destination address, IP protocol number, TCP/UDP source port number, TCP/UDP destination port number etc, then to proceed with certain actions like rate limit, prioritization or discard.

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

7.1.8 Security Management

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

- User management, including user name, passwords, etc.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of SSH for the communication between LMT clients and the TOE.
- Defining IP addresses and address ranges for clients that are allowed to connect to the TOE.

All of these management options are typically available via the LMT GUI.

Detailed function specification include following:

1) Support Local configuration through console port. Parameters include console port baud rate, data bit, parity, etc;
2) Support configuration for authentication and authorization on user logging in via console port;
3) Support configuration for authentication mode and authorization mode on user logging in via console port;
4) Support remotely managing the TOE using SSH.
5) Support enabling, disabling S-FTP;
6) Support configuration on service port for SSH;
7) Support configuration on RSA/DSA/ECC key for SSH;

8) Support configuration on authentication type, encryption algorithm for SSH;
9) Support authenticate user logged in using SSH, by password authentication, RSA/DSA/ECC authentication, or combination of both;
10) Support configuration on logout when no operation is performed on the user session within a given interval;
11) Support configuration on max attempts due to authentication failure within certain period of time;
12) Support configuration on limiting access by IP address;
13) Support configuration on commands' access level;
14) Support management on OSPF by enabling, disabling OSPF;
15) Support configuration on area, IP address range, authentication type of OSPF;
16) Support management on BGP by enabling, disabling BGP;
17) Support configuration on peer address, authentication type of BGP;
18) Support management on ARP by specifying static ARP entry, aging time and frequency of dynamical ARP entry. This function is achieved by interpreting commands input and storing value in memory.
19) Support management on log by enabling, disabling log output;
20) Support configuration on log output channel, output host;
21) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
22) Support enabling, disabling SNMP Agent and Trap message sending function;
23) Support enabling, disabling the switch to Send an Alarm Message of a Specified Feature to the NM Station ;
24) Support setting the Source Interface, Queue Length and Lifetime of Trap message;
25) Support enabling, disabling STP function .

Above functions are achieved by providing interpreting input commands and storing result of interpreting in memory. Some results like routes generated, ACLs will be downloaded into hardware to assist forwarding and other TSF functions. (FMT_SMF.1)

7.1.9 User Security

The TOE offers an Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces. The administrator can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against ACL rules specified. Source MAC address, Destination MAC address, Ethernet protocol type, Source IP address, destination IP

address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, type and code if ICMP protocol, fragment flag etc., can be used for ACL rule configuration.

To prevent attackers bypassing this ACL (and other attacks), the TOE also offers:

- **Port security** which checks whether the source MAC addresses of data frames received on an interface are valid and takes action if they are not.
- **DHCP snooping**, which intercepts and analyzes DHCP messages transmitted between DHCP clients and a DHCP server, and, from these messages DHCP snooping creates and maintains a DHCP snooping binding table, which is used by IP Source Guard and Dynamic ARP Inspection (see further). DHCP snooping also filters out messages from/to unauthorized DHCP servers.
- **IP Source Guard**, which the TOE uses to check IP packets against the DHCP snooping binding table and thereby filters out packets that do not match this table (and therefore have probably forged their IP address).
- **Dynamic ARP inspection** (DAI) allows the device to compare the source IP address, source MAC address, interface number, and VLAN ID of an ARP packet with the DHCP snooping binding table. If an entry is matched, the device considers the ARP packet valid and allows the packet to pass through. If no entry is matched, the device considers the ARP packet invalid and discards the packet.

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

7.1.10 Denial-of-Service Protection

The TOE uses two specific mechanisms to prevent Denial of Service against itself or the network it protects:

- **CPCAR** (Control Plane Committed Access Rate) limits the rate of protocol packets sent to the control plane and schedules the packets to protect the control plane. The switch identifies service packets based on ACLs and applies the default CAR value to protocol packets so that a limited number of protocol packets are sent to the control plane. Security of the control plane is ensured. CPCAR can be used to set the rate at which classes of packets are sent to the CPU, or the total rate of packets sent to the CPU. When the rate exceeds the upper limit, the system discards excess packets to prevent CPU overload
- **Traffic suppression** limits the number of unknown unicast packets, multicast packets, and broadcast packets within a proper range to ensure network efficiency. The TOE can suppress the packets based on interfaces and VLANs. When traffic suppression is enabled on an interface, the TOE checks whether the traffic volume of unknown unicast packets, multicast packets, and broadcast packets received by the interface monitors exceeds the threshold. If the traffic volume exceeds the threshold, the CloudEngine Series Switch discards excess packets to keep the traffic volume within the limit to ensure that services run properly.

  (FDP_IFC.1(1), FDP_IFF.1(1))

7.1.11 Cryptographic functions

Cryptographic functions are required by security features as dependencies. The following cryptographic algorithms are supported:

1) Support AES128/AES256/3DES/RSA/DSA/ECC algorithms. This is achieved by providing implementations of AES128/AES256/3DES/RSA/DSA/ECC algorithms.
2) Support MD5/HMAC-MD5/SHA2 algorithms. This is achieved by providing implementations of MD5/HMAC-MD5/SHA2 algorithms.
3) Support for RSA/DSA/ECC key construction and destruction overwriting it with 0

   (FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4/*)

7.1.12 Time

The TOE supports its own clock, to support logging and timed log-outs.

(FPT_STM.1, FTA_SSL.3)

7.1.13 SNMP Trap

The TOE uses SNMP traps to notify a fault occurs or the system does not operate properly.

1) Support management on trap by enabling, disabling trap output;
2) Support configuration on trap output interface, output host;
3) Support configuration on trap based on fault categories, fault functionality, or modules where the faults occur.
4) Support SNMPv3 which provides:
   a) Encrypted communication using DES，3DES, AES128, AES192, AES256 algorithm.
   b) Packet authentication using MD5/SHA algorithms

   (FTP_ITC.1, FDP_DAU.1)

7.1.14 STP

The TOE supports Spanning Tree Protocol (STP) to cut off the potential loops on the network and provide Link redundancy.

1) Support blocking a certain interface to prevent replication and circular propagation of packets on the network.
2) Support sending configuration BPDUs and Hello packets to detect link faults with a certain time.
3) Support delay for interface status transition to prevent transient loops.
4) Support configuration on max aging time to specifies the aging time of BPDUs, (FRU_FLT.1, FPT_FLS.1)

8 Abbreviations, Terminology and References

8.1 Abbreviations

ACL	Access Control List
CC	Common Criteria
CLI	Command Line Interface
GUI	Graphical User Interface
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MPU	Main Processing Unit
NTP	Network Time Protocol
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SNMP	Simple Network Management Protocol
SPU	Service Process Unit
SRU	Switch Router Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
VP	Virtual Path
VRP	Versatile Routing Platform

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal

context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

User: A user is a human or a product/application using the TOE.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation. September 2012. Version 3.1 Revision 4.