Huawei NetEngine AR6121 and AR6121E V300R019C13 Routers

Security Target

Version: V1.6

Last Update: 2023-05-11

Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2019-12-25	0.1	Initial Draft	Gu Zhenlin
2020-01-07	0.2	Modify	Gu Zhenlin
2020-03-17	0.3	Modify, update the IPSEC information	Gu Zhenlin
2020-06-05	0.4	Modify for comments	Gu Zhenlin
2020-06-29	0.5	Modify for comments(6-18)	Gu Zhenlin
2020-07-31	0.6	Delete MD5	Gu Zhenlin
2020-11-17	0.7	Update	Gu Zhenlin
2020-12-02	0.8	Update for comments	Gu Zhenlin
2021-02-02	0.9	Update for comments	Wang Chunning
2021-02-19	1.0	Update for comments	Wang Chunning
2021-08-30	1.1	Update for comments	Wang Chunning
2022-05-05	1.2	Update for comments	Wang Chunning
2022-06-29	1.3	Update for comments	Wang Chunning
2023-03-27	1.4	Update for comments	Xiong Ran
2023-05-09	1.5	Update for comments	Xiong Ran
2023-05-11	1.6	Update for comments	Xiong Ran

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of Huawei NetEngine AR6121 and AR6121E Routers.

1.1 Security Target Identification

Name:	Huawei NetEngine AR6121 and AR6121E, V300R019C13 Routers Security Target
Version:	1.6
Publication Date:	2023-05-11
Author:	Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name:	Huawei NetEngine AR6121and AR6121E Routers
Version:	V300R019C13
Developer:	HUAWEI Technologies Co., Ltd.

1.3 Target of Evaluation (TOE) Overview

The TOE type is a network device that is connected to the network and has an infrastructural role within the network.

Huawei NetEngine AR6121 and AR6121E Routers are network routing engines and gateway devices, which provide the routing, switching, wireless, and security functions. Huawei AR provides a highly secure and reliable platform for scalable multi-service integration at enterprise and commercial branch offices of all sizes and small-to-medium sized businesses. It consists of both hardware and software. AR6121 and AR6121E routers have identical software architecture. The only difference in physical architecture of AR6121 and AR6121E is the memory (SDRAM) capacity: AR6121E is equipped with 4GB SDRAM whereas AR6121 is equipped with 2GB SDRAM.

At the core of each router is the VRP (Versatile Routing Platform) deployed on MPU (Main Processing Unit) that include MCU (Main Control Unit) and SRU (Switch Routing Unit), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include access control; 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.

MCU (Main Control Unit) and SRU (Switch Routing Unit) are also providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP.

1.4 TOE Description

1.4.1 Architectural overview

This section will introduce the Huawei NetEngine AR6121 and AR6121E routers running VRP from a physical architectural and a software architectural point of view.

The TOE are Huawei AR 6121 and AR6121E Routers running Huawei VRP. A router is a device that determines the next network point to which a packet should be forwarded toward its destination. It is located at any gateway (where one network meets another). A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGP, RIP, ISIS and OSPF. IP packets are forwarded to the router over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the router. This processing typically results in the IP packets being forwarded out of the router over another interface.

Huawei AR6121 and AR6121E Routers use quadcore CPU processing capabilities, Control and management plane and data forwarding plane are in one board; but Core 0 is dedicated for control and management process, the other CPU cores are dynamically allocated to forwarding and service processes. In the software architectural, VRP uses VP (Virtual Path) to connect control plane, management plane and data forwarding plane.

1.4.1.1 Physical Architecture

1.4.1.1.1 Physical Architecture of Huawei AR6121 and AR6121E Routers

When the TOE is in use, at least two of the network interfaces of the internetworking device will be attached to different networks. The router configuration determines how packet flows received on an interface will be handled. Typically, packets are forwarded through the internetworking device and forwarded to their configured destination. Routing protocols used are RIP, OSPF, ISIS, and BGP.

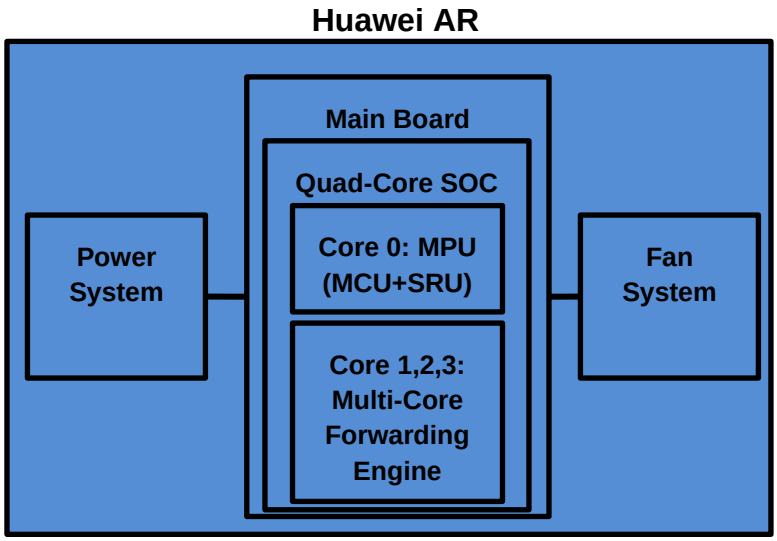

Figure 1: TOE Physical architecture of AR

Figure 1 shows the physical architecture of the TOE with the power and fan systems modules. The AR hardware provides the running environment, which includes the following systems:

- Power system
- Fan system
- Core 0 (MCU+SRU), for running Versatile Routing Platform (VRP)
- Other 3 Cores, for running forwarding Engine (Data Plane)

As shown in Figure 1, the main board mainly consists of an SOC chip with Quad-Core processing capability. In Core 0, the SRU+MCU are hosting the VRP which provides control and management functionalities. The other 3 cores in the SOC chip form the forwarding engine and are dynamically allocated for network traffic processing, the forwarding engine determines how packets are handled to and from the router's network interfaces. And generally SRU+MCU are called MPU for simplicity. The SRU+MCU and forwarding engine are running on an SOC chip, the independent core, hardware cache, parsing and distribution engine in the SOC form the forwarding engine.

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

1.4.1.2 Software Architecture

1.4.1.2.1 Software Architecture of AR

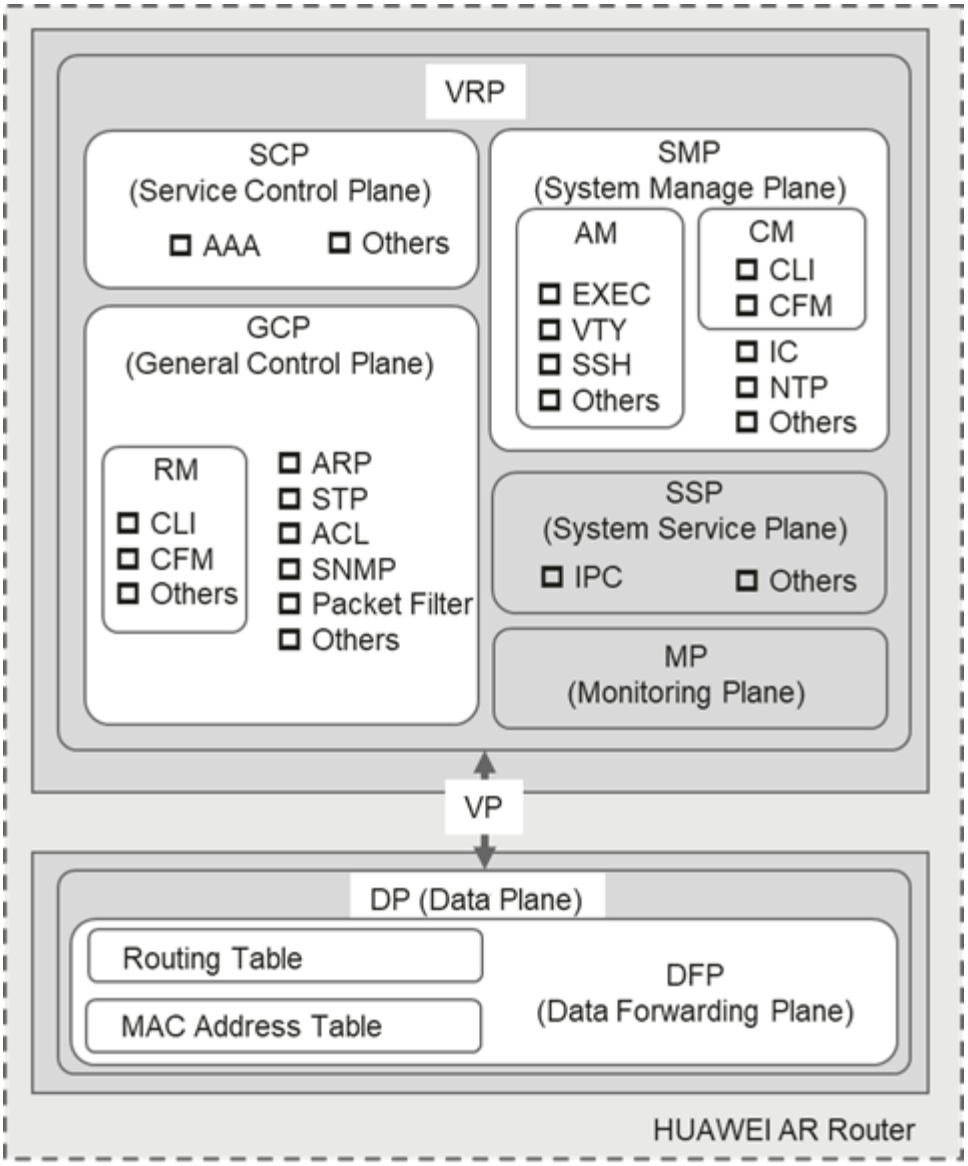

Figure 2: TOE Software architecture of AR

Figure 2 shows a brief illustration of the software architecture of the TOE. 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 (DFP, Routing table, MAC Address table)
- Control and management plane (SCP, SMP, GCP)
- System Service Plane (SSP) (Non-TSF)
- Monitoring plane (Non-TSF)

The **monitoring plane** (Non-TSF) monitors the system environment by detecting the voltage, controlling power-on and power-off of the system, and monitoring the

temperature and controlling the fan, and send an alarm to the customer while system overload occurs. For example, the fan speed increases when the temperature increases, and the fan speed decreases when the temperature decreases. When the temperature is too high or too low or the fan is faulty, the device sends an alarm.

The **System Service Plane** (SSP) (Non-TSF) provides the abstract layer of the operating system so that the VRP can be independent of the specific operating system.

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 **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.

1.4.2 Scope of Evaluation

The physical scope of evaluation is the Huawei NetEngine AR6121 and AR6121E routers. The logical scope of evaluation is defined in the following section.

1.4.2.1 Physical scope

This section will define the physical scope (Table 1) of the Huawei NetEngine AR6121 and AR6121E routers to be evaluated.

Both AR6121 and AR6121E are built with same hardware components. The only difference between AR6121 and AR6121E is the SDRAM capacity. AR6121 is equipped with 2GB SDRAM while AR6121E is equipped with 4GB SDRAM.

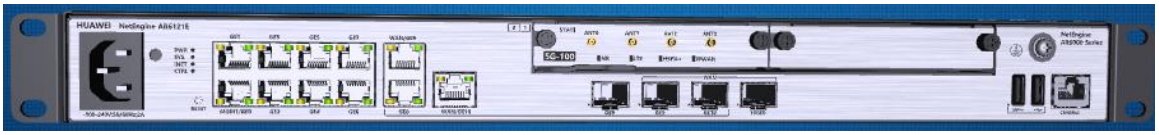

Figure 3-1: Appearance of AR6121 and AR6121E

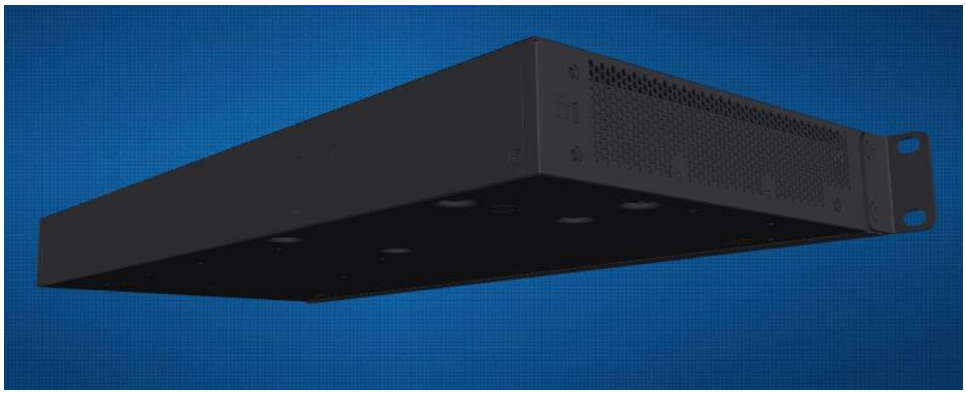

Figure 4-2: Appearance of AR6121 and AR6121E

The TOE deliverables are summarized in the following tables:

TYPE	Deliverables	Model Number / Version	Method of Delivery
Hardware	AR6121 and AR6121E Routers as shown in Table 2~3.	AR6121 and AR6121E	Logistic company appointed by Huawei
Software	AR6121 and AR6121E routers V300R019C13 Format: .cc binary file Filename :AR6120-V300R019C13SPCXXX.cc Info: Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature(The digital signature is also published on HUAWEI support website) -----BEGIN PGP SIGNATURE----- Version: GnuPG v2.0.19 (GNU/Linux) iQEcBAABCAAGBQJey4ZrAAoJEJmtgd8np0gkAjoH/1BRf3jB3nS5hCePWrRh9qgY No2kX8GCJXZZ8xPDxO5XcCcjE4cP+VaWhNktAQE1tlKr4uMKI8vRgvJ7FP/izeRQ fV20KRDvdwRoGzrCtRKZaiyBq/U8BHuWeU9jBgKry4UJQtSZZuOsIlWWDVrzz4VA XBOEAlUNuFD/eaO6DtOgThW1LvPb1rmWX+0Zi8rGxojFEkEjDFoEKVtmMQDJuy3x DebS/b4+Yu2qJlDIgLyKyj5g4K/G2/Aam1R4XklFIRehiJ7sgNSZcP8lwJySBqiU ZFfziD7yCgeFU36wxmDGf+GPyHlycCvyg8XeGPRUeP6wuT2MtshZm8O9WdnSOgY= =6n/b -----END PGP SIGNATURE-----	V300R019C13	Huawei support website (https://support.huawei.com/enterprise/en/index.html)
Product guidance	NetEngine AR V300R019 Product Documentation Format: webpage or .hdx (Huawei product documentation format, can be opened using HedEx Lite)	V300R019	Website: https://support.huawei.com/hedex/hdx.do?docid=EDOC1

TYPE	Deliverables	Model Number / Version	Method of Delivery
	Users can login the HUAWEI support website to view the documentation or download the document and open using HedEx Lite		100087043 &lang=en

Table 1: Deliverables of the TOE

Model Types	Typical System Configuration and Physical Parameters		
AR6121	**Item**	**Typical Configuration**	**Remark**
	Processing unit	1.4GHz 4Core	-
	SDRAM	2GB	-
	Flash	512M	-
	Forwarding Performance	3M pps	
	Fixed interface	GE/10GE	1*10GE+1*GE combo + 8*GE
	SIC Slot	2	
	WSIC Slot	0	
	XSIC Slot	0	
AR6121E	**Item**	**Typical Configuration**	**Remark**
	Processing unit	1.4GHz 4Core	-
	SDRAM	4GB	-
	Flash	512M	-
	Forwarding Performance	3M pps	
	Fixed interface	GE/10GE	1*10GE+1*GE combo + 8*GE
	SIC Slot	2	
	WSIC Slot	0	
	XSIC Slot	0	

Table 2: AR6121 and AR6121E Model Specifications

Boards	Supported Interfaces and Usage
MCU,SRU and Forwarding Engine	The following list shows a collection of interfaces which might be used during this evaluation. The description about indicators on panel can be found in user manual "***AR Hardware Description.pdf***". • ETH interface, connector type RJ45, operation mode 10M/100M/1000M/10000M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002, used for connections initiated by users and/or administrators from a local maintenance terminal via SSH (SSH2.0) to perform management and maintenance operations. Management and maintenance on NMS Workstation is not within the scope of this evaluation thus NMS related accounts should be disabled during the evaluation. • GE interface, connector type LC/PC optical connector, compliant to small form-factor pluggable optical module 1000Base-X, supporting full-duplex, used for receiving and transmitting network traffic. • Console interface, connector type RJ45, operation mode Duplex Universal Asynchronous Receiver/Transmitter (UART) with electrical attribute RS-232, baud rate 9600 bit/s which can be changed as required, used for users and/or administrators to connect to console for the on-site configuration of the system. • USB interface, connector type USB compatible with USB 2.0 standard used to hold a USB disk to store data files as a massive storage device.

Table 3: AR Interfaces Specifications

1.4.2.2 Logical scope

The elements in the Versatile Routing Platform (VRP) that are considered part of the TSF are displayed with white background in Figure 5. System Service Plane (SSP) and Monitoring Plane (MP) are considered as non-TSF.

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

Figure 5 shows the TOE's logical scope with supporting network devices of the environment. The TOE support external identification and authentication service, however this external service, as indicate below in Figure 4, the Radius and TACACS+ server authorization is not included in the evaluation scope.

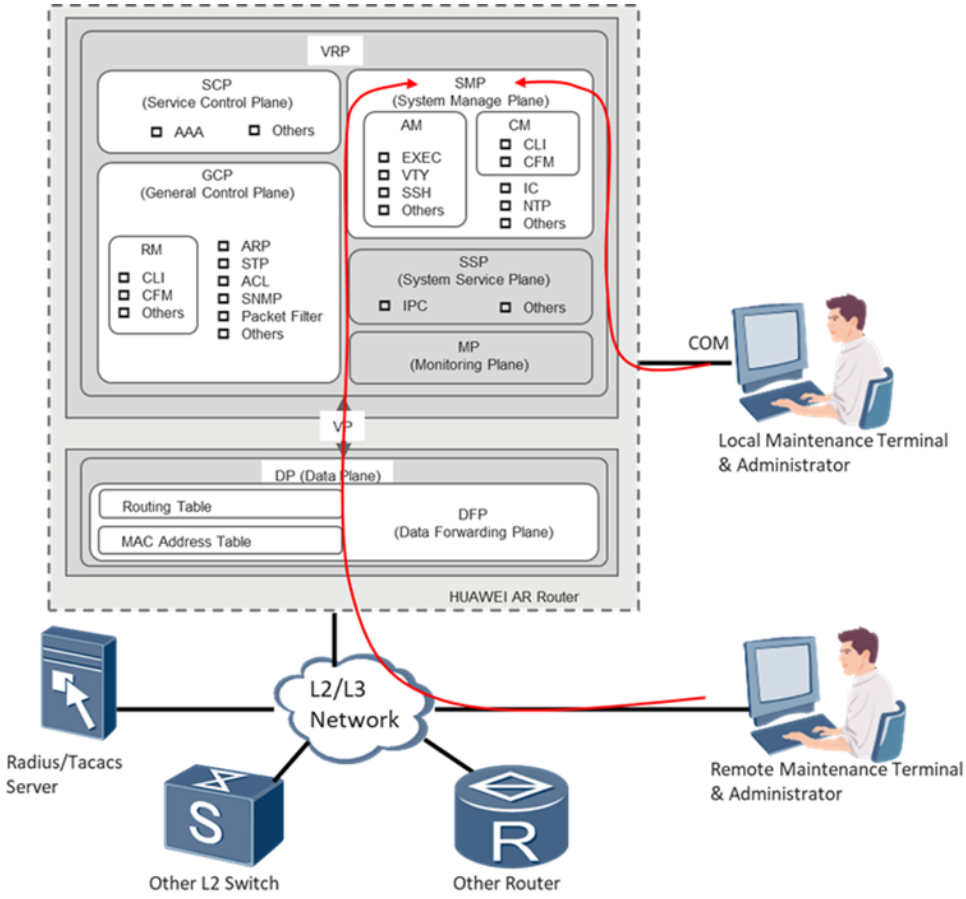

Figure 5: TOE logical scope

The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of IP packets against routing table in forwarding engine.

The TOE can be used for Layer 2 forwarding and Layer 3 forwarding purposes.

When working as Layer 2 forwarding devices, the forwarding engine of TOE will forward the traffic according to MAC address.

When working as Layer 3 forwarding devices，The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless 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 can be performed locally or remotely.

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

- To manage the TOE through the console interface, the administrator needs to connect the COM port of the PC to the console port of the TOE using a serial cable. Administrators can initialize configurations, such as IP addresses and VTY users.

This is a local management method. In this scenario, authentication is always enabled. The authentication mode is password, and the password contains at least eight characters.

- To manage the TOE through ETH interfaces, the administrator can connect the ETH interface of the PC to the ETH interface of the device through a Layer 2 or Layer 3 network. For management via the ETH interface in MCU+SRU, 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 (SSH2.0) connections is supported. SSH server compatible with version number less than 1.99 is considered a weakness, therefore will be disabled. By default, the RSA authentication mode is used for SSH users.

1.4.3 Summary of Security Features

1.4.3.1 Authentication

The TOE can authenticate administrative users by user name and password.

VRP provides a local authentication scheme for this.

Authentication is always enforced for virtual terminal sessions via SSH (SSH2.0), and S-FTP (Secured FTP) sessions. Authentication for access via the console is always enabled.

1.4.3.2 Access Control

The TOE controls access by levels. Four hierarchical administrative levels are offered that can be assigned to individual user accounts:

Administrative level	**Level name**	**Purpose**	**Commands for access**
0	Visit	Network diagnosis and establishment of remote connections.	ping, tracert, language-mode, super, quit, display
1	Monitoring	System maintenance and fault diagnosis.	Level 0 and display, debugging, reset, refresh, terminal, send
2	Configuration	Service configuration.	Level 0, 1 and all configuration commands.
3 to 15	Management	System management (file system, user	All commands.

Administrative level	Level name	Purpose	Commands for access
		management, internal parameters …).	

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. Radius and TACACS+ server authorization is not included in the evaluation scope.

1.4.3.3 L2 Traffic Forwarding

The TOE handles layer 2 forwarding policy at its 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.

1.4.3.4 L3 Traffic Forwarding

The TOE handles forwarding policy at its 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.

The TOE support IPsec protocol. By authenticating and encrypting each IP packet in the data flow, the IP datagram is provided with high-quality, interoperable, and password-based security.

1.4.3.5 Auditing

VRP generates audit records for security-relevant management actions and stores the audit records in flash in the TOE.

- By default all correctly input and executed commands along with a timestamp when they are executed are logged.
- Attempts to access regardless success or failure is logged, along with user id, source IP address, timestamp etc.
- For security management purpose, the 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.
- The TOE supports Network Time Protocol (NTP) client mode and it relies on NTP server to provide a reliable time source.

1.4.3.6 Communication Security

The TOE provides communication security by implementing SSH protocol. SSH2 (SSH2.0) is implemented. SSH2 is used for all cases by providing more secure and effectiveness in terms of functionality and performance,

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH2 provides:

- authentication by password, by RSA or by password with RSA;
- AES encryption algorithms
- Secure cryptographic key exchange by DH-group14-sha256
- HMAC-SHA256 is used as verification algorithm for SSH2.

S-Telnet and S-FTP are provided to implement secure Telnet and FTP, as alternatives to Telnet and FTP which are deemed to have known security issues. The S-Telnet is implemented by SSH2.

The TOE provides IPsec protocol to protect IP packets forwarding. IPsec is a supplement to IP security. It works at the IP layer to provide transparent security services for IP network communication. IPsec provides:

- Key-exchange: Group 14(2048 bits) and Group 21(521-bits ECP)
- AES-CBC-256 encryption algorithms.
- Integrity: hmac-sha2-512
- Digital Signature: PSS and PKCS1

1.4.3.7 ACL

TOE offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces.

The administrator can create, delete, and modify rules in 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 that specified in the ACL rules. 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 is in use), destination port number (if TCP/UDP protocol is in use), TCP flag (if TCP protocol is in use), type and code (if ICMP protocol is in use), fragment flag etc, can be used for ACL rule configuration. If no rule is created in an ACL, the ACL cannot match any traffic.

If no ACL or ACL rule is configured, the TOE performs the following operations based on features:

1. For filtering features (such as Telnet), if no ACL is configured, login is allowed

by default.

2. By default, the prioritize and rate-limit are not adjusted and the original forwarding mode is used.

1.4.3.8 Security functionality management

Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

More functionalities include:

- Setup to enable SSH2.0
- Setup to enable BGP, OSPF, ARP
- Setup to enable audit, as well as suppression of repeated log records
- Setup to change default rate limit plan

In addition to management of TSF, the TOE also supports Network event report using Simple Network Management Protocol (SNMP). It is capable of reporting an occurrence of a fault. 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 NMS 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 NMS Workstation.

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

1.4.3.9 Cryptographic functions

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

1. AES256 is used as default encryption algorithm for SSH2
2. RSA is used in user authentication when user tries to authenticate and gain access to the TOE
3. SHA256 is used as option HMAC algorithm for SSH2
4. HMAC-SHA256 is used as verification algorithm for packets of BGP and OSPF protocols from peer network devices

1.4.3.10 Packet Filtering

Packet Filtering is the primary functionality implemented by the TOE. The packet filtering filters packets through ACLs. It is based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.

TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), in order to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE, the TOE applies an information flow security policy in the form of access control lists and stateful inspection to the traffic before forwarding it into the remote network. Packet flows arriving at a network interface of the TOE are checked to ensure that they conform with the configured packet filter policy, this may include checking attributes such as the presumed source or destination IP address, the protocol used, the network interface the packet flow was received on, and source or destination UDP/TCP port numbers. Packet flows not matching the configured packet filter policy are dropped.

1.4.4 TSF and Non-TSF data

All data from and to the interfaces available on the TOE is categorized into TSF data and non-TSF data. The following is an enumeration of the subjects and objects participating in the policy.

TSF data:

- User account data, including the following security attributes:
  - User identities.
  - Locally managed passwords.
  - Locally managed access levels.
- Audit configuration data.
- Audit records.
- Configuration data of security feature and functions
- Routing and other network forwarding-related tables, including the following security attributes:
  - Network layer routing tables.
  - Link layer address resolution tables.
  - Link layer MAC address table.
  - BGP, OSPF databases.
- Network traffic destined to the TOE processed by security feature and functions.

Non-TSF data:

- Network traffic to be forwarded to other network interfaces.
- Network traffic destined to the TOE processed by non-security feature and functions.

1.4.5 TOE type

The TOE type is a network device that is connected to the network and has an infrastructure role within the network.

1.4.6 Non TOE Hardware and Software

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being “Required” or “Optional” based on the claims made in this Security Target. All of the following environment components are supported by the TOE in its evaluated configurations.

Components	**Required/ Optional**	**Usage/Purpose Description for TOE performance**
Switches and routers	Required	Used to connect the TOE for L2/L3 network forwarding. L3 switches provide routing information to the TOE via dynamic protocols such as BGP and OSPF.
Local NMS Workstation	Required	This includes any Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration. In some simple environments, a local console is required. The local console allows administrators to perform initial configurations, such as IP addresses or user accounts.
Remote NMS Workstation	Required	This includes any Management workstation with a SSH client installed that is used to establish a protected channel with the TOE.
Physical network	Required	Such as Ethernet subnets, interconnecting various networking devices.
NTP Server	Required	NTP server provides reliable and trusted time source.

Table 5: IT Environment Components

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. There are no extended components defined – neither for CC Part 2 nor for CC Part 3. The CC version of is 3.1R5.

No conformance to a Protection Profile is claimed.

This ST is conforming to assurance package EAL2 augmented with ALC_FLR.2.

3 TOE Security problem definition

3.1 Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below.

3.1.1 Threats

T.UnwantedL2NetworkTraffic	A potential attacker might target the L2 network traffic by sending unwanted L2 network traffic to the TOE and it cause the MAC table gets updated dynamically by MAC learning function. This may cause the MAC table overload. In the TOE 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.
T.UnwantedL3NetworkTraffic	A potential attacker might target the L3 network traffic by sending unwanted L3 network traffic to the TOE. This will not only consumes the TOE's processing capacity for incoming network traffic and results in failure to process the traffic it is expected to handle; but also give rise to a potential internal traffic jam when those traffic are sent to the Control Plane. Routing information exchanged between the TOE and peer routes may also be affected due the traffic overload.
T.UnauthenticatedAccess	Potential attackers or unauthenticated users may exploit weak authentication implementation to gain access to the TOE.

	Consequently, the TOE configuration data might be modified and results in compromised TOE integrity.
T.UnauthorizedAccess	A malicious user of the TOE might attempt to exploit a weak authorization implementation to gain access to TSF configurations and its data. This might compromise the TSF and hence the TOE integrity.
T.Eavesdrop	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and LMT/RMT.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.PhysicalProtection It is assumed that the TOE (including any console attached, access flash) is protected against unauthorized physical access.

3.2.1.2 Network Elements

A.NetworkElements The environment is supposed to provide supporting mechanism to the TOE:

- Peer router(s) for the exchange of dynamic routing information;
- A local PC for TOE administration;
- A remote entities (PCs) used for administration of the TOE;
- Physical network which provides network connection to the TOE;
- NTP server for providing reliable time source

3.2.1.3 Network Segregation

A.NetworkSegregation It is assumed that the ETH interface in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separated from the application (or, public) networks.

3.2.1.4 Authorized Administrators

A.NoEvil The authorized administrators are well-trained and understand the TOE security functionalities. They are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Forwarding** The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a configured route for the destination IP address of the packet, or corresponds with a MAC address for the destination MAC address of the packet. When TOE works as Layer 2 forwarding

device, traffic should be isolated between VLANs. TOE should supported stateful packet filtering, defend against network attacks.

- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- **O.Authentication** The TOE must authenticate users of its user access.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.Resource** The TOE shall provide functionalities and management for assigning a priority (used as configured bandwidth) , enforcing maximum quotas for bandwidth and priority.
- **O.Filter** The TOE shall provide ACL or packet filter to drop unwanted L2 or L3 network traffic.

4.2 Objectives for the Operational Environment

- **OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other routers for the exchange of routing information, PCs used for TOE administration and NTP server for providing reliable time source.
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the ETH interface in TOE into a local sub-network, compared to the network interfaces in TOE serving the application (or public) network.
- **OE.Person** Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

Objective	Threat
O.Forwarding	T.UnwantedL2NetworkTraffic T. UnwantedL3NetworkTraffic
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	T.UnauthenticatedAccess T.UnauthorizedAccess
O.Resource	T.UnwantedL2NetworkTraffic T.UnwantedL3NetworkTraffic
O.Filter	T.UnwantedL2NetworkTraffic T.UnwantedL3NetworkTraffic

Table 6: Mapping Objectives to Threats

The following table provides a mapping of the objectives for the operational environment to assumptions, threats and policies, showing that each objective is at least covered by one assumption, threat or policy.

Environmental Objective	Threat / Assumption
OE.NetworkElements	A.NetworkElements T.UnauthenticatedAccess T.UnauthorizedAccess
OE.Physical	A.PhysicalProtection
OE.NetworkSegregation	A.NetworkSegregation
OE.Person	A.NoEvil

Table 7: Mapping Objectives for the Environment to Threats, Assumptions

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat,

when achieved, actually contributes to the removal of that threat:

Threat	Rationale for security objectives to remove Threats
T.UnwantedL2NetworkTraffic	The L2 layer traffic should be isolated between VLANs. (O.Forwarding) MAC address limit configuration can avoid the overload of MAC table entry caused by fake MAC address attack that can cause exhaustion of forwarding resources.(O.Resource) ACL or Packet filter can deny unwanted L2 network traffic enter or pass TOE to protect the TOE resource. (O.Filter)
T.UnwantedL3NetworkTraffic	The threat that unwanted network traffic sent to TOE causing the TOE a management failure and internal traffic jam is countered by specifying static routes to filter those traffic (O.Forwarding). ACL can also be configured to filter those traffic that can cause exhaustion of TOE resources. (O.Resource). ACL or Packet filter can deny unwanted L3 network traffic enter or pass TOE to protect the TOE resource. (O.Filter)
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 tracing of possible culprits. The TOE also relies upon NTP server in its operational environment to provide reliable time stamp for logging purposes (O.Audit and OE.NetworkElements)
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, login attempts are logged allowing detection of attempts and tracing of possible culprits. The TOE also relies upon NTP server in its operational environment to provide reliable time stamp for logging purposes (O.Audit and OE.NetworkElements)

Threat	Rationale for security objectives to remove Threats
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSH (protocol v.2) protocol for network communication between LMT/RMT and the TOE. To avoid middle man attacks, public server key is pre-loaded to client (O.Communication).

Table 8: Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each assumption, and each security objective for the environment could be traced back to at least an assumption on the environment of use of the TOE. If the security objectives for the environment are achieved, it will result in an operational environment that is consistent with the assumption, and the intended usage of the TOE is supported:

Assumption	Rationale for security objectives
A.NetworkElements	The assumption that the external network devices such as peer router for routing information exchange, LMT/RMT for TOE control and management and NTP server for providing reliable time source are addressed in OE.NetworkElements.
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access is expressed by a corresponding requirement in OE.Physical.
A.NetworkSegregation	It is assumed that the ETH interface on MPU in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks where the interfaces on Interface boards in the TOE are accessible.
A.NoEvil	The authorized users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Table 9: Sufficiency analysis 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 TOE 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 group 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)**, **Remote NMS 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 **users authorized per FDP_ACF.1** 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 **log level, slot-id, regular-expression.**

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 8 MB.**

6.2.2 Cryptographic Support (FCS)

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 in CTR and CBC mode** and cryptographic key sizes **that is configurable up to 256 bits** that meet the following: **FIPS 197.**

6.2.2.2 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **asymmetric authentication** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **configured (2048bits-4096bits, default value is 2048 bits)** that meet the following: **RSA Cryptography Standard (PKCS#1)**

6.2.2.3 FCS_COP.1/HMAC Cryptographic operation

FCS_COP.1.1 The TSF shall perform **authentication** in accordance with a specified cryptographic algorithm **HMAC-Sha2-256** and cryptographic key sizes **256 bits** that meet the following: **ISO/IEC 9797-2:2011**

6.2.2.4 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-group14-sha256** and cryptographic key sizes **diffie-hellman-group14-sha256: 2048 bits, Diffie-hellman-group-21: 521-bit ECP (Elliptic Curve Groups modulo a Prime)** that meet the following: **RFC 4419/RFC 3526/RFC 5114/ RFC 5903.**

6.2.2.5 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 **diffie-hellman-group-14-sha256/diffie-hellman-group-21** and specified cryptographic key sizes **2048 bits (DH-group-14-sha256)/521-bit ECP (DH-group-21)** that meet the following: **RFC 4419/RFC 3526/RFC 5114/RFC 5903.**

6.2.2.6 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 **SSH2 key derivation** and specified cryptographic key sizes **256bits** that meet the following: **RFC 4253**

6.2.2.7 FCS_CKM.1/HMAC_SHA256 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSH2 key derivation** and specified cryptographic key sizes **256 bits** that meet the following**: RFC 6668**

6.2.2.8 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 keygen method **RSA** and specified cryptographic key sizes **configured (2048bits)** that meet the following: **RSA Cryptography Standard (PKCS#1)**

6.2.2.9 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**

6.2.2.10 FCS_CKM.4/HMAC_SHA256 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**

6.2.2.11 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 **overwriting with 0** that meets the following: **none**

6.2.2.12 FCS_CKM.4/AES 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 **users as subjects, and commands as objects.**

Application Note: TOE access control SFP is defined in Section 1.4.3.1 and 1.4.3.2 in the [ST]. Basically the subjects covered by the SFP are users; the objects covered by the SFP are commands; and the information security attributes are user level and command groups.

User level: Range from 0 to 15. Higher user level offers higher privilege and access.

Command groups: By default, there are 4 command groups range from 0 to 3. For each command, the level can be configured by administrator (value range from 0 to 15). Refer to Table 4 in [ST] for details on the association of command groups to user access level.

The VRP access control SFP restrict the access of a user to certain commands. For a command, only user with a user level that is higher or equal to the command level have access to that particular command.

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:

a) users and their following security attributes:

1. User level

b) commands and their following security attributes:

1. Command Groups

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) the user has been granted authorization for the commands targeted by the request, and

b) the user is associated with a Command Group that contains the requested command

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 commands targeted by the request, and

b) the user is associated with a Command Group that contains the requested command

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, and

b) the user is not associated with a Command Group that contains the requested command

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, SSH2, NTP,SNMP**

FDP_DAU.1.2 The TSF shall provide **the authentication processes in BGP, OSPF, SSH2, NTP,SNMP** with the ability to verify evidence of the validity of the indicated information.

6.2.3.4 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce **the VRP information control policy(based on ACL)** on **the subject as network traffic, the ACL-defined information, the ACL-defined operations**.

Application Note: The information flow control policy is enforced by ACL feature of the TOE, as defined in Section 1.4.3.7 in the [ST]. The subjects covered by the SFP are network packets. And the information security attributes are source MAC address, Destination MAC address, Ethernet protocol types, Source IP address, destination IP address, destination port number (for TCP/UDP protocol), TCP flag, type and code, fragment flag etc.

6.2.3.5 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **VRP information control policy (based on ACL)** based on the following types of subject and information security attributes: **the subject as network packets or frames, the information security attributes as source IP address, destination IP address, transport protocol, source TCP or UDP port number, destination TCP or port number, ICMP types or flags, source MAC address, destination MAC address**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the VRP information control policy, and the policy's action is permit**.

FDP_IFF.1.3 The TSF shall enforce the **bandwidth control, traffic statistic**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **the VRP information control policy, and the policy's action is permit**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **VRP information control policy, and the policy's action is deny**.

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 related to **since the last successful authentication of the indicated user identity**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***surpassed***, the TSF shall **terminate the session of the user trying to authenticate and block the user account for at least 5 minutes.**

Application Note: If an incorrect user name or password is entered, the device adds the IP address of the user to the blocklist. The IP address is locked for 2 seconds after the first login failure, 4 seconds after the second login, and 8 seconds after the third login failure. If the user enters incorrect user names or passwords for five consecutive times, the IP address is locked for 300 seconds after the sixth login failure.

During the lockout period, the blocklisted IP addresses cannot be used to establish connections through new windows. After the lockout period expires, if you enter the correct user name and password for login, the IP address is removed from the blocklist and the restoration log is recorded. If the login fails again, the system will be locked for 300 seconds.

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
d) Unsuccessful authentication attempt since last successful authentication attempt counter(default: 3 attempts)
e) Login start and end time.

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 HMAC-SHA256 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 8 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 HMAC-SHA256 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 8 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 HMAC-SHA256 authentication for SNMP, 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 8 to 64 characters.**

FIA_SOS.1.1/d The TSF shall provide a mechanism to verify that secrets meet **for password used as seeds for HMAC-SHA256 authentication for NTP, 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 6 to 16 characters.**

FIA_SOS.1.1/e The TSF shall provide a mechanism to verify that secrets meet **for password used as seeds for HMAC-SHA256 authentication for SSH2 and they are case sensitive. A cipher password mode should be used and the length of password should be at least 8 characters long.**

6.2.4.4 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.5 FIA_UID.2 User identification before any action

FIA_UID.2.1 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*** the functions **defined in FMT_SMF.1** to **the administrator-defined roles**.

Application Notes: Administrator-defined roles means the user accounts granted privilege to operate TSF by administrator.

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 **Control Plane Committed Access Rate (CPCAR)/Blacklist** to restrict the ability to ***query, modify, delete*** the security attributes **identified in FDP_IFF.1** to **the roles which can match the Control Plane Committed Access Rate (CPCAR)/Blacklist and the policy action is permit**.

Application Note CPCAR(Control Plane Committed Access Rate). With the CPU attack defense function, the device limits the rate of packets sent to the CPU to protect the CPU.

Reference:
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100087043&lang=en&idPath=24030814|21432787|23708834|250680700

Configuration->CLI-based Configuration->Security Configuration Guide->Local Attack Defense Configuration

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 ***permissive*** default values for security attributes (Command Group associations) that are used to enforce the SFP.

Application Note: Refer to Section 1.4.3.2 for details on command group associations

FMT_MSA.3.2/1 The TSF shall allow **administrator-defined roles** to specify alternative initial values to override the default values when an object or information is created.

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.3.2/2 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 policy
b) ACL policy
c) user management
d) definition for Command Groups
e) definition of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests
f) routing and forwarding, such as BGP, OSPF, ARP
g) L2 forwarding, such as MAC, VLAN

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.

6.2.7 Resource utilization (FRU)

6.2.7.1 FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority (based on maximum packet rate) to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to **packet rate** shall be mediated on the basis of the subjects assigned priority.

6.2.7.2 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resource: **packet rate, MAC address table entries** that ***subjects*** can use ***simultaneously*****.**

6.2.8 TOE access (FTA)

6.2.8.1 FTA_SSL.3 TSF-initiated termination

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

Application Note: 0 to 35791 minutes, 0 indicates no timeout. Default user connection timeout interval is 5 minutes

6.2.8.2 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.

6.2.9 Trusted Path/Channels (FTP)

6.2.9.1 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***.

Application Note: Local user connect to the TOE via console port, which is only accessible if the user is given privilege to access to the premise where the TOE is physically located.

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

Application Note: Remote user connect to the TOE is via secure communication, which is only accessible either SFTP over SSH2 or STELNET over SSH2.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***initial user authentication, remote administration of TOE.***

6.3 Security Functional Requirements Rationale

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Security Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.3	O.Audit
FAU_STG.1	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC, FCS_COP.1/DHKeyExchange	O.Communication O.Authentication
FCS_CKM.1/AES, FCS_CKM.1/RSA, FCS_CKM.1/HMAC_SHA256, FCS_CKM.1/DHKey	O.Communication
FCS_CKM.4/AES, FCS_CKM.4/RSA, FCS_CKM.4/HMAC_SHA256, FCS_CKM.1/DHKey	O.Communication
FDP_ACC.1	O.Authorization O.Forwarding
FDP_ACF.1	O.Authorization O.Forwarding
FDP_DAU.1	O.Authentication O.Forwarding
FDP_IFC.1	O.Filter

Security Functional Requirements	Security Objectives
FDP_IFF.1	O.Filter
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication
FIA_UAU.2	O.Authentication O.Forwarding
FIA_UID.2	O.Audit O.Authentication O.Authorization O.Forwarding
FMT_MOF.1	O.Authorization
FMT_MSA.1	O.Authorization O.Filter
FMT_MSA.3	O.Authorization O.Filter
FMT_SMF.1	O.Audit O.Authentication O.Authorization O.Communication O.Filter
FMT_SMR.1	O.Authorization
FRU_PRS.1	O.Resource
FRU_RSA.1	O.Resource
FTA_SSL.3	O.Authentication O.Authorization
FTA_TSE.1	O.Authentication
FTP_TRP.1	O.Communication O.Forwarding

Table 10: Mapping SFRs to Security Objectives

6.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the

security objectives:

Security objectives	Rationale
O.Forwarding	The goal of secure traffic forwarding is achieved by following: Prior to forwarding related service configuration, authentication (FIA_UAU.2, FDP_DAU.1, FIA_UID.2), authorization (FDP_ACC.1) and access control policy (FDP_ACF.1) are implemented and applicable. A trusted path (FTP_TRP.1) for forwarding related service configuration should be established for users.
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp (OE.NetworkElements) and user identities (FAU_GEN.2) where applicable, which are supplied by the authentication mechanism (FIA_UID.2). Audit records are in a string format, regular expressions are provisioned to read and search these records (FAU_SAR.1, FAU_SAR.3). The protection of the stored audit records is implemented in FAU_STG.1. Functionality to delete the oldest audit file is provided if the size of the log files becomes larger than the capacity of the store device (FAU_STG.3). Management functionality for the audit mechanism is spelled out in FMT_SMF.1.
O.Communication	Communications security is implemented by the establishment of a secure communications channel, and a trusted path for remote users in FTP_TRP.1. FCS_COP.1 addresses the AES encryption of SSH (SSH2.0) channels. FCS_CKM.1 addresses keys generation of AES/RSA. FCS_CKM.4 addresses key destruction of RSA. Note that keys of AES algorithms are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination. The allocated memory is freed as well. Management functionality to enable these mechanisms is provided in FMT_SMF.1.
O.Authentication	User authentication is implemented by FIA_UAU.2, FDP_DAU.1 and supported by individual user identifies in FIA_UID.2. The necessary user attributes (passwords) are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for logon (FTA_TSE.1), and a

Security objectives	Rationale
	password policy (FIA_SOS.1). Management functionality is provided in FMT_SMF.1. Logging out users after an inactivity period (FTA_SSL.3). Provide the cryptographic services for the authentication (FCS_COP.1)
O.Authorization	The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. Unique user IDs are necessary for access control provisioning (FIA_UID.2), and user-related attributes are spelled out in FIA_ATD.1. Access control is based on the definition of roles as subject and functions as object (FMT_SMR.1, FMT_MOF.1), The termination of an interactive session is provided in FTA_SSL.3. Management functionality for the definition of access control policies is provided (FMT_MSA.1, FMT_MSA.3, FMT_SMF.1).
O.Resource	The requirement for assigning a priority (used as configured bandwidth) is spelled out in FRU_PRS.1, enforcing the maximum quotas for bandwidth and limited the MAC address table entries is spelled out in FRU_RSA.1
O.Filter	The requirement of ACL or packet filter is spelled out in FDP_IFF.1 and FDP_IFC.1. management functionality for the definition of ACL is provided (FMT_MSA.1, FMT_MSA.3, FMT_SMF.1).

Table 11: SFR sufficiency analysis

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 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	Satisfied by OE.NetworkElements. The TOE cannot provide reliable time stamps. Reliable time stamps must be provided by the Operational Environment.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
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
FCS_COP.1/AES	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/AES FCS_CKM.4/AES
FCS_COP.1/RSA	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/RSA FCS_CKM.4/RSA
FCS_COP.1/HMAC-SHA256	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/HMAC_SHA256 FCS_CKM.4/HMAC_SHA256
FCS_COP.1/DHKeyExchange	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DHKey FCS_CKM.4/DHKey
FCS_CKM.1/AES	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/AES FCS_CKM.4/AES
FCS_CKM.1/RSA	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/RSA FCS_CKM.4/RSA
FCS_CKM.1/DHKey	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DHKeyExchange FCS_CKM.4/DHKey
FCS_CKM.1/HMAC_SHA256	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/HMAC_SHA256 FCS_CKM.4/HMAC_SHA256
FCS_CKM.4/AES	[FDP_ITC.1, or	FCS_CKM.1/AES

Security Functional Requirement	Dependencies	Resolution
	FDP_ITC.2, or FCS_CKM.1]	
FCS_CKM.4/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA
FCS_CKM.4/HMAC_SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/HMAC_SHA256
FCS_CKM.4/DHKey	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/DHKey
FAU_STG.3	FAU_STG.1	FAU_STG.1
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	None	
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	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 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Security Functional Requirement	Dependencies	Resolution
FRU_PRS.1	None	
FRU_RSA.1	None	
FTA_SSL.3	None	
FTA_TSE.1	None	
FTP_TRP.1	None	

Table 12: Dependencies between TOE Security Functional Requirements

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 2 augmented with ALC_FLR.2, 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

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 when user login via SSH (SSH2.0), which include password authentication, RSA authentication, or combination of both. This function is achieved by performing authentication for SSH user based on method mentioned in 1).
3) 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.
4) Support max attempts due to authentication failure within certain period of time (default 5 minutes - configurable). This function is achieved by providing counts on authentication failure.
5) Support limiting access by IP address. This function is achieved by comparing IP address of requesting session with configured value stored in memory.
6) Support locking operation interface. This function is achieved by storing lock/unlock state in memory, and performing authentication when state is lock.
7) Support manual session termination by username. This function is achieved by interpreting commands for username, locating and cleaning session information related to this username, forcing this username to re-authenticate.
8) Support for user individual attributes in order to achieve all the enumerated features: user ID, user level, password, unsuccessful authentication attempt since last successful authentication, attempt counter and login start and end time.

(FCS_COP.1/RSA, FDP_DAU.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2, 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 4 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.
5) Support creating blacklist by ACL. The device will discard the packets matched ACLs.
6) Support setting different rates or discard different types of packets (CPCAR rate configuration) to reduce the number of packets sent to the CPU and protect the CPU.

(FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_MOF.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 limit the learning number of MAC address
6) Support to convert the MAC address learnt dynamically to static MAC address
7) Support MAC address flapping protection
8) In order to configure all the settings, the user must be an authenticated administrator with sufficient access rights.
9) The TOE supports Spanning Tree Protocol (STP) to cut off the potential loops on the network and provide Link redundancy.

   (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 IP addresses and MAC addresses:

1) Support ARP/ OSPF/BGP protocol. This function is achieved by providing implementation of ARP /OSPF/BGP 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 HMAC-SHA256. This function is achieved by performing verification for incoming BGP packets using HMAC-SHA256. algorithm.
8) OSPF support cryptographic algorithm HMAC-SHA256.. This function is achieved by performing verification for incoming OSPF packets using HMAC-SHA256. 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 LPU in the TOE. If it is, the traffic will be sent to VRP in MCU for central process.

15) Only administrators can configure L3 traffic forwarding information. Authentication is required before you configure and view L3 traffic forwarding information.

16) Support IPsec. By authenticating and encrypting each IP packet in the data flow, the IP datagram is provided with high-quality, interoperable, and password-based security. It supports AES encryption algorithm for cipher, supports Group14 and Group21 for key exchange, supports hmac-sha2-512 for integrity, and supports RSA for digital signature.

(FIA_UAU.2, FTP_TRP.1, 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. Log channel for output is selected prior to execution of redirecting.

4) Support log output screening, based on severity level, regular expression. This function is performed by providing filtering on output.

5) Support multiple log file format: binary, readable text. This function is achieved by providing output format transformation.

6) Support querying log buffer. This function is achieved by performing querying operation with conditions input.

7) Support cleaning log buffer. This function is achieved by cleaning log buffer in memory.

8) Support to automatically remove oldest log files if audit files exceed the size of store device.

9) Only the authorized administrators can monitor the logfile record, and operate the log files. The unauthorized users have no access to do those actions. And the actions of the authorized administrators will be logged.

10) Allows all authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for reading audit records) to

read the audit records.

11) Does not support unauthorized modification of audit information.

12) Restricts the ability to delete audit event information to authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for deleting audit records).

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

7.1.6 Communication Security

The TOE provides communication security by implementing SSH protocol (SSH2.0). The

SSHv2 (SSH2.0) is implemented. SSH2 is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance. S-Telnet and S-FTP are provided implementing secure Telnet and FTP, to substitute Telnet and FTP which are deemed to have known security issues.

1) Support SSHv2. This function is achieved by providing implementation of SSHv2.

2) Support diffie-hellman-group14-sha256, as key exchange algorithm of SSH2. This function is achieved by providing implementation of diffie-hellman-group14-sha256 algorithm.

3) Support AES encryption algorithm. This function is achieved by providing implementation of AES algorithm.

4) Support HMAC-SHA2-256 verification algorithm. This function is achieved by providing implementation of HMAC-SHA2-256 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 S-TELNET. This function is achieved by providing implementation of S-TELNET.

7) Support S-FTP. This function is achieved by providing implementation of Secure-FTP.

(FMT_SMF.1, FDP_DAU.1)

7.1.7 ACL

The TOE supports Access Control List (ACL) to filter traffic destined to TOE to prevent internal traffic overload and service interruption. And the TOE also use ACL to deny unwanted network traffic to pass through itself.

The TOE also uses the ACL to identify flows and perform flow control to prevent the CPU and related services from being attacked.

1) Support enabling ACLs by associating ACLs to whitelist, blacklist, user-defined-flow. This function is achieved by interpreting ACL configurations then storing interpreted value in memory.
2) Support screening, filtering traffic destined to CPU. This function is achieved by downloading blacklist ACL configurations into hardware.
3) Support rate limiting traffic based on screened traffic. This function is achieved by downloading configuration of rate into hardware.

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

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 (unsecure if disabled).
- 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 and RMT 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 remotely managing the TOE using SSH (SSH2.0). SSH (SSH2.0) is required. Otherwise, security cannot be maintained.
4) Support enabling, disabling S-Telnet/S-FTP;
5) Support configuration on service port for SSH (SSH2.0);
6) Support configuration on RSA key for SSH (SSH2.0);
7) Support configuration on authentication type, encryption algorithm for SSH (SSH2.0);

8) Support authenticate user logged in using SSH (SSH2.0), by password authentication, RSA authentication, or combination of both;
9) Support configuration on logout when no operation is performed on the user session within a given interval;
10) Support configuration on max attempts due to authentication failure within certain period of time;
11) Support configuration on limiting access by IP address;
12) Support configuration on commands' access level;
13) Support management on OSPF by enabling, disabling OSPF;
14) Support configuration on area, IP address range, authentication type of OSPF;
15) Support management on BGP by enabling, disabling BGP;
16) Support configuration on peer address, authentication type of BGP;
17) 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.
18) Support management on log by enabling, disabling log output;
19) Support configuration on log output channel, output host;
20) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
21) Support configuration on operation modes of NTP;
22) Support configuration on authentication for NTP client and server by HMAC-SHA256 password;
23) Support enabling, disabling SNMP Agent and Trap message sending function;
24) Support enabling, disabling the switch to Send an Alarm Message of a Specified Feature to the NM Station ;
25) Support setting the Source Interface, Queue Length and Lifetime of Trap message;
26) Support configuration packet filtering based on ACL

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 Cryptographic functions

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

1) Supports symmetric encryption and decryption using the AES algorithm in CTR mode according to [FIPS 197] and [FIPS SP 800-38A] using key lengths that is configurable up to 256bits. AES in CTR mode is used for encryption and decryption within SSH (SSH2.0) communication.
2) Supports asymmetric authentication of the server to the client using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 using a key length of 2048bits. RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication for SSH (SSH2.0) according to chap. 6.6 [RFC 4253], ssh-rsa. The TOE supports asymmetric authentication of the client to the TOE (server) using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 using a key length of 2048bits. RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication for SSH (SSH2.0) according to chap. 7 [RFC 4252], 'publickey'.
3) Supports hashing of data using HMAC_SHA256 algorithm according to [FIPS 180-4].
4) Supports a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented in the field of cryptography. The Diffie-Hellman key exchange method allows two parties without prior knowledge of each other to jointly establish a shared secret key through an insecure communication channel. This key can then be used to encrypt subsequent communications using symmetric key cryptography.
5) Supports the generation of cryptographic keys according to diffie-hellman-group14-sha2 and specified cryptographic key sizes 2048bits according to [RFC 4253], [RFC 3526], [PKCS#3] for SSH (SSH2.0). The TOE generates a shared secret value with the client during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption (AES-in CTR mode) and generation and verification of integrity protection information (HMAC-SHA2) for SSH (SSH2.0) communication. The key generation is performed according to [RFC 4253], chap. 7.2.
6) Supports the generation for AES algorithm according to [FIPS 197].AES keys generated have a key length that is configurable up to 256 bit. AES in CBC mode is used for IPSec.

7) Supports the generation for HMAC_SHA256 algorithm according to [RFC 4634],[FIPS 180-2] using key lengths of 256bit. HMAC_SHA256 is uses for IPSec.
8) Supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT. RSA keys generated have a key length of 2048bits and are intended for usage with RSASSA-PKCS1-V1_5.
9) Support for key destruction, overwriting it with 0.

(FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC, FCS_COP.1/DHKeyExchange, FCS_CKM.1/DHKey, FCS_CKM.1/AES, FCS_CKM.1/HMAC_SHA256, FCS_CMK.1/RSA, FCS_CMK.4/RSA, FCS_CKM.4/HMAC_SHA256, FCS_CKM.4/DHKey, FCS_CKM.4/AES)

7.1.10 Packet Filtering

The TOE performs packet filtering by applying an information flow security policy, in the form of access control lists and stateful inspection, to specific interfaces of the TOE-enabled router.

1) Support ACL rule, which is based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.
2) The TOE shall permit an information flow between controlled subjects if all information security attributes are permitted by ACL. Packets not matching the ACL are logged and discarded by the router.
3) Support stateful packet filter, the stateful packet filter monitors the TCP/UDP sessions by using various status tables. The sessions matching the ACL can be established. Only the data packets associated with the allowed sessions are forwarded.

(FDP_IFC.1, FDP_IFF.1)

8 Crypto Disclaimer

The following cryptographic algorithms are used by AR6121 to enforce its security policy:

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Key Generation	RSA schemes	-	2048-bits~4096-bits, default value is 2048 bits	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3	FCS_CKM.1/RSA
2	Key Establishment	diffie-hellman-group-21		512-bits ECP	RFC 5903	FCS_CKM.1/DH Key
		diffie-hellman-group-14-sha256		2048-bits	RFC 3526	
3	Confidentiality	AES in CTR mode		Configurable up to 256 bits	AES as specified in ISO 18033-3, CTR as specified in ISO 10116	FCS_COP.1/ AES
4	Authentication	RSA signature	RSA: PKCS#1_V2.1, RSASSA-PKCS2v1_5	3072 bits	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5	FCS_COP.1/ RSA
			Digital signature scheme 2 or Digital Signature scheme 3	3072 bits	ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	FCS_COP.1/ RSA
	Integrity	HMAC-SHA-256	-	256 bits	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”	FCS_COP.1/HMAC
5	Cryptographic Primitive	SHA-256,	-	256 bits	ISO/IEC 10118-3:2004	FCS_COP.1/ DHKeyExchange
7	Trusted Channel	SSH V2.0	RFC 4251 RFC 4252 RFC 4253 RFC 4254 RFC 5656	-	-	FTP_TRP.1/ Admin

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
			RFC 6668			
8	Cryptographic Primitive	Generation of prime numbers for RSA	None			Miller-Rabin-Test is used as primality test.

Table 13: Algorithms in security policy

9 Abbreviations, Terminology and References

9.1 Abbreviations

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

NTP	Network Time Protocol
ACL	Access Control List
SNMP	Simple Network Management Protocol
NMS	Network Management System
SCP	Service Control Plane
SMP	System Manage Plane
GCP	General Control Plane
VTY	Virtual Teletype

9.2 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.

Operator See User.

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

9.3 References

As defined by the references [CC1], [CC2] and [CC3], this ST:

- conforms to the requirements of Common Criteria v3.1, Revision 5
- does not claim conformance to any other PP than the one specified in chap 2.2

Referenced Documents

[FIPS 186-4] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication FIPS PUB 186-4, July 2013

[PKCS#1] RSA Cryptography Specifications Version 2.1(RFC3447)

[PKCS#3] A cryptographic protocol that allows two parties that have no prior

knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

[FIPS 198-1]The Keyed-Hash Message Authentication Code (HMAC)--2008 July

[RFC 4251]The Secure Shell (SSH) Protocol Architecture, January 2006

[RFC 4252]The Secure Shell (SSH) Authentication Protocol, January 2006

[RFC 4253]The Secure Shell (SSH) Transport Layer Protocol, January 2006

[RFC 4254]The Secure Shell (SSH) Connection Protocol, January 2006

[RFC 6668]SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol

[RFC 3268]Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)

[RFC 4346]The Transport Layer Security (TLS) Protocol Version 1.1

[RFC 5246]The Transport Layer Security (TLS) Protocol Version 1.2

[RFC 8446]The Transport Layer Security (TLS) Protocol Version 1.3

[RFC 6125]Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)

[NIST SP 800-56A]National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013

[NIST SP 800-56B]National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography August 2009

[ISO/IEC 18031:2011] Information technology -- Security techniques -- Random bit generation

[ISO 18033-3] Information technology — Security techniques — Encryption algorithms

[ISO/IEC 9796-2]Information technology -- Security techniques -- Digital signature schemes giving message recovery

[ISO/IEC 9797-2]Information technology -- Security techniques -- Message Authentication Codes (MACs)

[ISO/IEC 10118-3]Information technology -- Security techniques -- Hash-functions

[ISO/IEC 14888-3] Information technology -- Security techniques -- Digital signatures with appendix.