Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target

Version: 0.68
Last Update: 2011-02-24
Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2010-08-20	0.40	Initial Draft	Weijianxiong Dusheng
2010-10-10	0.50	Adapt ST to CC V3.1 template	Weijianxiong Dusheng
2011-01-07	0.56	Fix observation note	Weijianxiong Dusheng
2011-01-31	0.59	Fix observation note	Dusheng
2011-02-16	0.63	Fix notes regarding ST identification, TOE identification, and chapter 6	Weijianxiong Dusheng
2011-02-18	0.65	Fix notes regarding functional specification	Weijianxiong Dusheng
2011-02-21	0.66	Fix notes regarding functional specification, and some content in chapter 6	Weijianxiong Dusheng
2011-02-23	0.67	Add font style convention to chapter 6	Dusheng
2011-02-24	0.68	Revise interface desc for LPU in chap 1.4.2.1	Dusheng

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of Huawei NetEngine40E/CX600 Universal Service Router V600R001.

1.1 Security Target Identification

Name: Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target

Version: 0.68

Publication Date: 2011-02-24

Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei NetEngine40E/CX600 Universal Service Router

Version: V600R001

Chassis: NE40E-X16 / CX600-X16 VRP software Version 5 Release 7 with the following identifier (VRPV500R007C00SPC000), where 000 is the patch; Forwarding Engine software Version 6 Release 1 with the following identifier (V600R01C00SPC800), where 800 is the patch;
Chassis: NE40E-X8 / CX600-X8 VRP software Version 5 Release 7 with the following identifier (VRPV500R007C00SPC000), where 000 is the patch; Forwarding Engine software Version 6 Release 1 with the following identifier (V600R01C00SPC800), where 800 is the patch;
Chassis: NE40E-X3 / CX600-X3 VRP software Version 5 Release 7 with the following identifier (VRPV500R007C00SPC000), where 000 is the patch; Forwarding Engine software Version 6 Release 1 with the following identifier (V600R01C00SPC800), where 800 is the patch;
Chassis: NE40E-8 / CX600-8 VRP software Version 5 Release 7 with the following identifier (VRPV500R007C00SPC000), where 000 is the patch; Forwarding Engine software Version 6 Release 1 with the following identifier (V600R01C00SPC800), where 800 is the patch;
Chassis: NE40E-4 / CX600-4 VRP software Version 5 Release 7 with the following identifier (VRPV500R007C00SPC000), where 000 is the patch; Forwarding Engine software Version 6 Release 1 with the following identifier (V600R01C00SPC800), where 800 is the patch;

Sponsor: Huawei

Developer: Huawei

Certification ID:

Keywords: Huawei, VRP, Versatile Routing Platform, Service Routers

1.3 Target of Evaluation (TOE) Overview

Huawei NetEngine40E/CX600 Universal Service Router V600R001, the TOE, provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware and software.

At the core of each router is the Versatile Routing Platform (VRP) deployed on board Main Processing Unit (MPU) or Switch Routing Unit (SRU), 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.

The Line Processing Units (LPU) are the actual hardware 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 NetEngine40E/CX600 Universal Service Router V600R001 from a physical architectural view and a software architectural view.

1.4.1.1 Physical Architecture

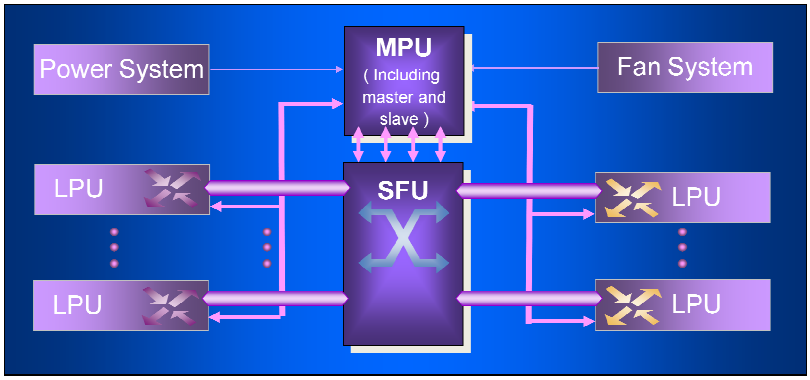

Figure 1: TOE Physical architecture

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

- Power distribution system
- Functional host system
- Heat dissipation system
- Network management system

Except the network management system (NMS), all the other systems are in the integrated cabinet. The power distribution system works in 1+1 backup mode. The functional host system is the target of this evaluation and following introductions will focus on the functional host system only. The Network management system, power distribution system and heat dissipation system are not within the scope of this evaluation.

The functional host system is composed of the system backplane, SRUs/MPUs, LPUs, and SFUs. SRU/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. Generally SRU/MPU are called MPU for simplicity in case of brief introduction.

The functional host system processes data. In addition, it monitors and manages the entire system, including the power distribution system, heat dissipation system, and NMS through NMS interfaces which are not within the scope of this evaluation.

1.4.1.2 Software Architecture

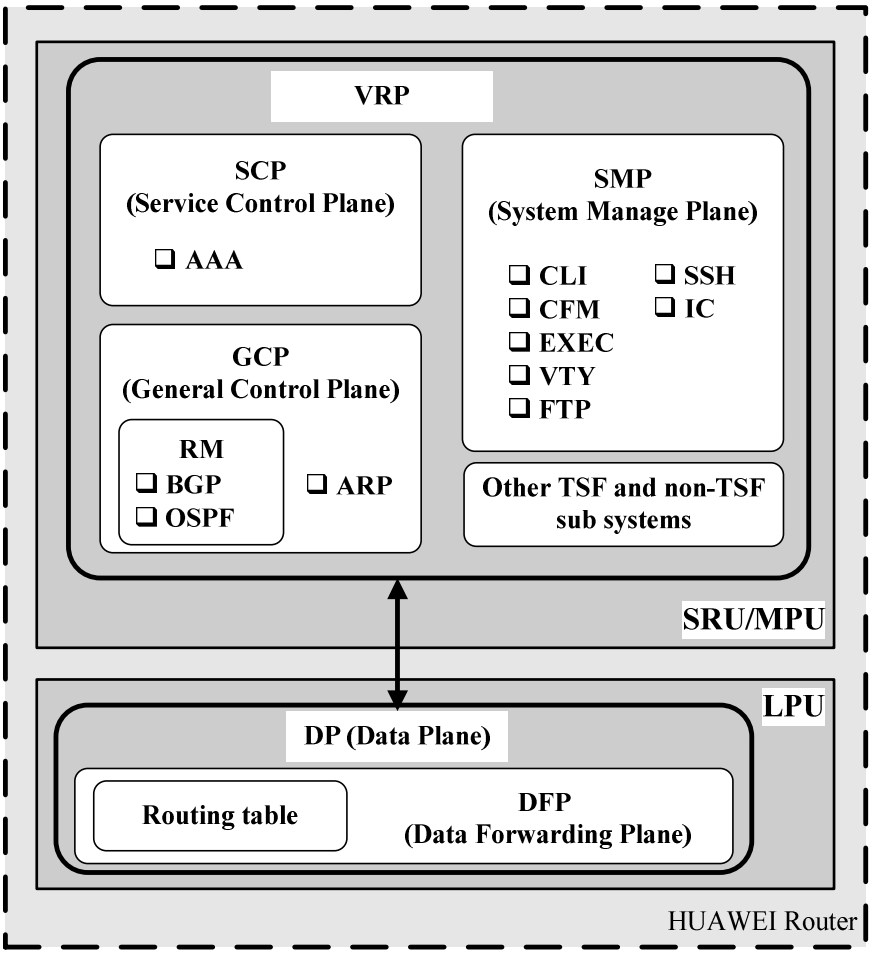

Figure 2: TOE Software architecture

In terms of the software, the TOE's software architecture consists of three logical planes to support centralized routing 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 security-related thus will not be further covered.

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.

Figure 2 shows a brief illustration of the software architecture of the TOE.

The VRP is the control and management platform that runs on the SRU/MPU. 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 Manage Plane (SMP), General Control Plane (GCP) and other TSF, non-TSF sub-systems.

The LPU implements the functions of the link layer and IP protocol stacks on interfaces and performs hardware-based IPv4/IPv6 forwarding, multicast forwarding and statistics.

1.4.2 Scope of Evaluation

This section will define the scope of the Huawei NetEngine40E/CX600 Universal Service Router V600R001 to be evaluated.

1.4.2.1 Physical scope

The physical boundary of the TOE is the actual router system itself -- in particular, the functional host system. The Network management system is not within the scope of this evaluation. The power distribution system and heat dissipation system are part of the TOE but not to be evaluated because they are security irrelevant.

The TOE provides several models. These models differ in their modularity and throughput by supplying more slots in hosting chassis, but they offer exchangeable forwarding unit modules, switch fabrics, and use the same version of software. The following models will be covered during this evaluation:

Model Types	Typical System Configuration and Physical Parameters		
NE40E-X16 CX600-X16	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.5 GHz	-
	BootROM	8 MB	-
	SDRAM	2 GB	Can be extended to 4 GB
	NVRAM	4 MB	-
	Flash	32 MB	-
	CF card	2 GB	Two CF cards, each of which is 1 GB
	Switching capacity	2.56 Tbit/s (bidirectional)	-
	Interface capacity	1.28 Tbit/s (bidirectional)	-

	Max MPU slots	2	-
	Max LPU slots	16	-
	Max SFU slots	4	-
NE40E-X8 CX600-X8	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.5 GHz	-
	BootROM	8 MB	-
	SDRAM	2 GB	Can be extended to 4 GB
	NVRAM	4 MB	-
	Flash	32 MB	-
	CF card	2 GB	Two CF cards, each of which is 1 GB
	Switching capacity	1.44 Tbit/s	-
	Interface capacity	640 Gbit/s (bidirectional)	-
	Max SRU slots	2	-
	Max LPU slots	8	-
	Max SFU slots	1	-
NE40E-X3 CX600-X3	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1 GHz	-
	BootROM	1 MB	-
	SDRAM	2 GB	-
	NVRAM	512 KB	-
	Flash	32 MB	-
	CF card	1 GB	-
	Switching capacity	1.08 Tbit/s	-
	Interface capacity	240 Gbit/s (bidirectional)	-
	Max MPU slots	2	-
	Max LPU slots	3	-
NE40E-8 CX600-8	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1 GHz	-

		BootROM	1 MB	-
		SDRAM	1 GB	Can be extended to 2 GB
		NVRAM	512 KB	-
		CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
		Switching capacity	640 Gbit/s	-
		Interface capacity	320 Gbit/s	-
		Max SRU/MPU slots	2	SRU/MPUs work in 1:1 redundancy.
		Max LPU slots	8	-
		Max SFU slots	2	SFUs work in 3+1 load balancing mode with the two SFU modules integrated into the SRU.
		Maximum interface rate per LPU	10 Gbit/s	-
NE40E-4 CX600-4		**Item**	**Typical Configuration**	**Remark**
		Processing unit	Main frequency: 1 GHz	-
		BootROM	1 MB	-
		SDRAM	1 GB	Can be extended to 2 GB
		NVRAM	512 KB	-
		CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
		Switching capacity	320 Gbit/s	-
		Interface capacity	160 Gbit/s	-
		Max SRU/MPU slots	2	SRU/MPUs work in 1:1 redundancy.
		Max LPU slots	4	-

	Max SFU slots	2	SFUs work in 3+1 load balancing mode with the two SFU modules integrated into the SRU.
	Maximum interface rate per LPU	10 Gbit/s	-

Table 1 Model Specifications

Table 2 details all physical interfaces available in TOE along with respective usage:

Boards	Supported Interfaces and Usage
MPU/SRU	The following list shows a collection of interfaces which might be used during this evaluation for all models. The description about indicators on panel can be found in user manual “CC NetEngine40ECX600 V600R001 - Hardware Description.pdf”. • CF card interface, connector type TYPE II compatible with TYPE I, is used to hold a CF card to store data files as a massive storage device. The CF card is inserted and sealed within the TOE and is to be accessed only by authorized personnel. User configuration profiles, paf and licensing files, log data, system software and patches if exist are stored in the CF card. • ETH interface, connector type RJ45, operation mode 10M/100M/1000M 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 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. • 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. The following interfaces if available according to hardware specification, will be disabled during this evaluation. • 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. • CTL-ETH-SFP interface (1000MBase-X), connector type SFP, reserved for usage after capacity expansion. Disabled during this evaluation. • AUX interface, connector type RJ45, used to connect to Model for remote maintenance through dialing. Disabled during this evaluation. • CLK/TOD0 and CLK/TOD1, connector type RJ45, used to input or output 2-Mbit/s clock signals, 2-MHz clock signals, 1pps+ASCII clock signals, or two channels of DCLS clock signals. Disabled during this evaluation.

	• CLK/1PPS, connector type SMB, used to input or output 2-Mbit/s clock signals, 2-MHz clock signals, or 1 PPS signals. Disabled during this evaluation. • CLK/Serial, connector type SMB, used to input or output 2-Mbit/s clock signals, 2-MHz clock signals, or RS232 signals. Disabled during this evaluation. • BITS0 and BITS1 interface, connector type RJ45, used for External synchronous clock/time interface • CLK-IN1 and CLK-IN2, connector type SMB, used to receive external 2-Mbit/s clock signals, 2-MHz clock signals. • CLK-OUT1 and CLK-OUT2, connector type SMB, used to output 2-Mbit/s clock signals, 2-MHz clock signals.
LPU	Interfaces supported by LPU are listed as below. More details about these interfaces can be found in user manual “CC NetEngine40ECX600 V600R001 - Hardware Description.pdf”, chapter C “List of LPU Interface Attributes”. • ETH interface, connector type RJ45, operation mode 10M/100M/1000M Base-TX auto-sensing, supporting half-duplex and full-duplex, used for receiving and transmitting network traffic. • FE interface, connector type LC/PC optical connector, compliant to SFP optical module 100M-FX, supporting full-duplex, used for receiving and transmitting network traffic. • GE interface, connector type LC/PC optical connector, compliant to SFP optical module 1000Base-X-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • 10GE interface, connector type LC/PC optical connector, compliant to XFP optical module 10GBase LAN/WAN-XFP, supporting full-duplex, used for receiving and transmitting network traffic The following interfaces are supported by the TOE, but not to be evaluated in this evaluation. • cPOS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-3c/STM-1 cPOS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-3c/STM-1c POS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-12c/STM-4c POS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • POS interface, connector type LC/PC optical connector, compliant to SFP optical module OC-48c/STM-16c POS-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • POS interface, connector type LC/PC optical connector, compliant to XFP optical module OC-192c/STM-64c POS-XFP, supporting full-duplex, used for receiving and transmitting network traffic. • ATM interface, connector type LC/PC optical connector, compliant to SFP optical module OC-3c/STM-1c ATM-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • ATM interface, connector type LC/PC optical connector, compliant

	to SFP optical module OC-12c/STM-4c ATM-SFP, supporting full-duplex, used for receiving and transmitting network traffic. • CE1/CT1 interface, connector type CE1/CT1, supporting full-duplex, used for receiving and transmitting network traffic. • E3/T3 interface, connector type SMB, supporting full-duplex, used for receiving and transmitting network traffic. The network traffic being received and transmitted by these interfaces, can be further described as non-TSF data (information flow to be forwarded to other network interfaces and information flow destined to TOE but not security-related) and TSF data (destined to TOE for control and management purpose and for security-related functionalities). The definition for non-TSF data and TSF data will be further explained in Chapter 1.4.4.

Table 2 Interfaces Specifications

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

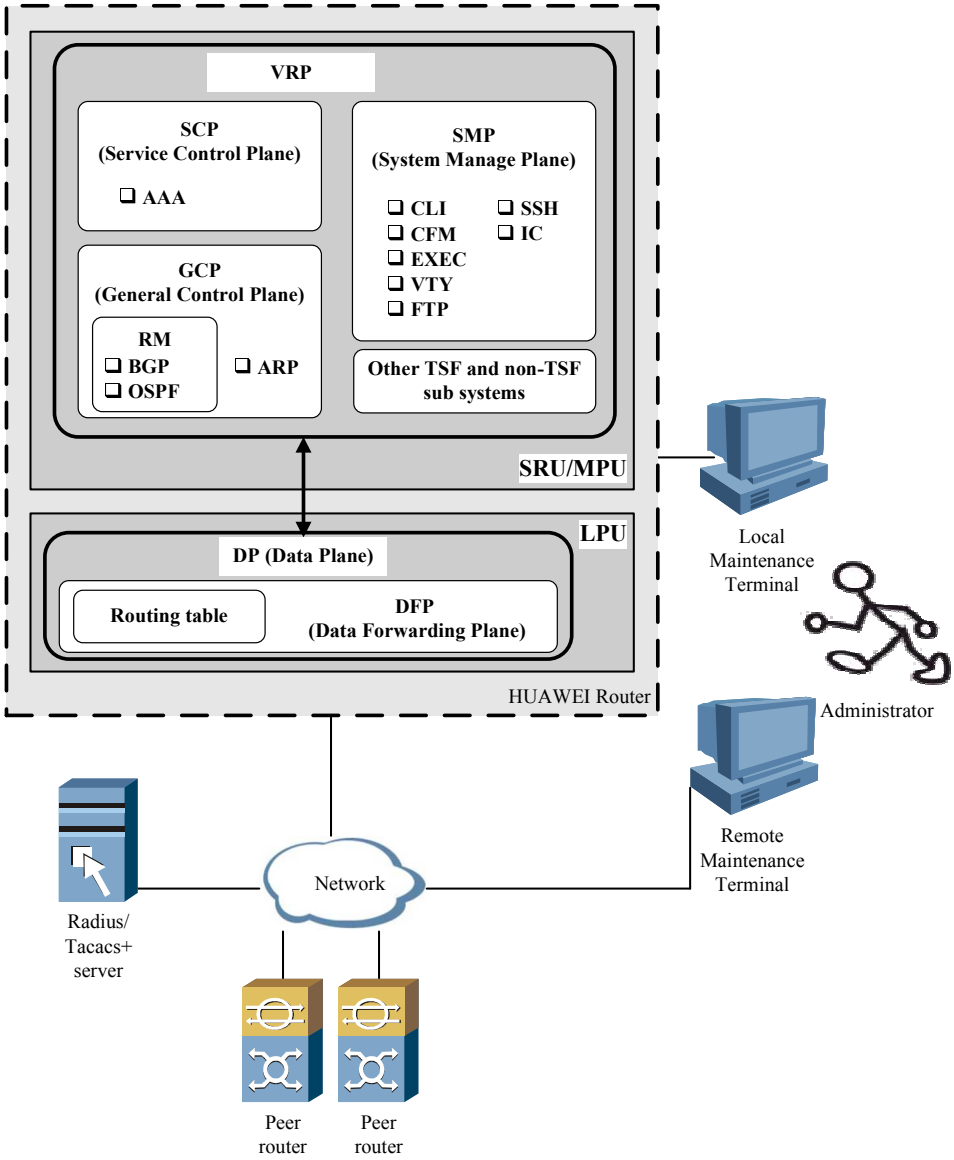

Figure 3: TOE logical scope

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). Note that BGP/OSPF functionality configuration must be performed via s secure channel enforcing SSH prior to routing table importing.

System control and security managements are performed either through interfaces on MPU/SRU or interfaces on LPU via a secure channel enforcing SSH.

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

- Connections via the router's AUX interface is not supported in this evaluated configuration thus AUX interface is disabled during this evaluation.

- For management via the console, authentication is always enabled.
- For management via the ETH interface, authentication is always enabled.
- Service of TELNET and FTP are disabled in this evaluation.
- Authentication of users via RSA when using SSH connections is supported.
- The method of using SNMP to apply configuration changes is not supported thus SNMP is disabled during this evaluation.
- Internal clock module is used as the system clock source. External clock source such as NTP time service, is not supported in this evaluated configuration.

The environment for TOE comprises the following components:

- An optional Radius or TACACS+ server providing authentication and authorization decisions to the TOE.
- Peer routers 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

1.4.3.1 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. Authentication for access via the console is always enabled.

1.4.3.2 Access Control

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

User 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	Configurat	Service configuration.	Level 0, 1 and all

User level	Level name	Purpose	Commands for access
	ion		configuration commands.
3	Managem ent	System management (file system, user management, internal parameters, …).	All commands.

Table 10: 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.

If no authentication for the console is configured, it operates at level 3.

1.4.3.3 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 that is either maintained by administrators (static routing) or gets updated dynamically by the TOE when exchanging routing information with peer routers.

1.4.3.4 Auditing

VRP generates audit records for security-relevant management actions And stores the audit records in CF card inserted into 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.

1.4.3.5 Communication Security

The TOE provides communication security by implementing SSH protocol. Two versions of SSH: SSH1 (SSH1.5) and SSH2 (SSH2.0) are implemented. But SSH2 is recommended for most 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, SSH provides:

- authentication by password and by RSA;
- 3DES/AES encryption algorithms;
- Secure cryptographic key exchange.

Besides default TCP port 22, manually specifying a listening port is also implemented

since it can effectively reduce attack.
STelnet and SFTP are provided implementing secure Telnet and FTP, to substitute Telnet and FTP which are deemed to have known security issues.

1.4.3.6 IP-based ACL

VRP offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces on LPU. Information flow that is processed with ACL and to be forwarded to other network interfaces is not within the scope of the evaluated configuration. Outgoing information flow processed with ACL towards other network interfaces is not within the scope of the evaluated configuration.

The administrator can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE through interfaces on LPU by matching information contained in the headers of connection-oriented or connectionless IP packets against ACL rules specified. 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.

1.4.3.7 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 SSH
- 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

1.4.3.8 Cryptographic functions

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

1) AES128 is used as default encryption algorithm for SSH;
2) 3DES is used as optional encryption algorithm for SSH;
3) RSA is used in user authentication when user tries to authenticate and gain access to the TOE;
4) MD5 is used as option HMAC algorithm for SSH;
5) MD5 is used as verification algorithm for packets of BGP and OSPF protocols from peer network devices;
6) HMAC-MD5 is used as verification algorithm for packets of SSH protocols.

1.4.3.9 Clock function

The MPU in TOE integrates clock module as the system clock source. It can provide the LPUs with 2.048 MHz synchronous clock signals.

Management of clock function by commands via CLI is provided. Date and time, daylight saving hour and time zone can all be adjusted by the user commands. Querying of time is also implemented by providing API on time-related functions.

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.
    - 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.

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R3.

This ST is EAL3-conformant as defined in [CC] Part 3.

No conformance to a Protection Profile is claimed.

3 TOE Security problem definition

3.1 Threats

The assumed security threats are listed below.

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.

As a result, the following threats have been identified:

- Unwanted network traffic A user who is not a user of the TOE is able to send network traffic to the TOE that the TOE is not supposed to process.
- Unauthenticated Access A user who is not a user of the TOE gains access to the TOE.
- Unauthorized Access An unauthorized personnel either attacker or authenticated user is able to gain access to TSF functionality that he is not authorized for.
- Traffic eavesdropped 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 .

3.1.1 Threats

T.UnwantedNetworkTraffic	Unwanted network traffic sent to the TOE will not only cause the TOE's processing capacity for incoming network traffic is consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to MPU from LPU within the TOE. This may further cause the TOE fails to respond to system control and security management operations. Routing information exchanged between the TOE and peer routes may also be affected due the traffic overload.
T.UnauthenticatedAccess	A user who is not a user of the TOE gains access to the TOE.
T.UnauthorizedAccess	A user of the TOE 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) 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 of CF card) 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: • A Radius server or TACACS+ server for external authentication/authorization decisions; • Peer router(s) for the exchange of dynamic routing information; • A remote entities (PCs) used for administration of the TOE.

3.2.1.3 Network Segregation

A.NetworkSegregation	It is assumed that the ETH interface on MPU/SRU 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 LPU in the TOE are accessable.

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 address of the packet.
- **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 configuration to prevent internal collapse due to traffic overload.

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. For example, other routers for the exchange of routing information, PCs used for TOE administration, and Radius and TACACS+ servers for obtaining authentication and authorization decisions.
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console, and CF card inserted in the MPU) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the Ethernet interface on MPU/SRU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.

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.UnwantedNetworkTraffic
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess
O.Authorization	T.UnauthorizedAccess

O.Audit	T.UnauthenticatedAccess T.UnauthorizedAccess
O.Resource	T.UnwantedNetworkTraffic

Table 4: 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
OE.Physical	A.PhysicalProtection
OE.NetworkSegregation	A.NetworkSegregation

Table 5: 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, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.UnwantedNetworkTraffic	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). IP-based ACL can also be configured to filter those traffic (O.Resource).
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).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSH protocol for network communication between LMT/RMT and the TOE (O.Communication).

Table 6: Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment

of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.NetworkElements	The assumption that the external network devices such as Radius server as an external authentication/authorization source, peer router for routing information exchange, and LMT/RMT for TOE control and management 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	The assumption that the TOE is not accessible via the application networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation.

Table 7: 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.

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)**, **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.**

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 store device.**

6.2.1.7 FPT_STM.1 Reliable time stamps

FPT_STM.1 The TSF shall be able to provide reliable time stamps.

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 **AES128** and cryptographic key sizes **128 bits**

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** and cryptographic key sizes **168 bits** 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 **RSA** and cryptographic key sizes **configured (1024bits-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 **none** that meet the following: **RFC 2104**

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 **diffie-hellman-group1-sha1/diffie-hellman-group-exchange-sha1** and specified cryptographic key sizes **128 bits** that meet the following: **RFC 4253/RFC 4419**

6.2.2.7 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 **diffie-hellman-group1-sha1/diffie-hellman-group-exchange-sha1** and specified cryptographic key sizes **56/168 bits** that meet the following: **RFC 4253/RFC 4419**

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 (1024bits-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**

6.2.3 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 issued by the subjects targeting the objects.**

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:

O. **user level**

b) commands and their following security attributes:

O. **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

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**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***surpassed***, 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

d) unsuccessful authentication attempt since last successful authentication attempt counter

e) login start and end time.

6.2.4.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

a) For character sequence used as seeds for OSPF/BGP, they are case sensitive and contain no whitespace, no question mark. The length of the character sequence for OSPF should be less than 8 characters. In other cases the length should be less than 16 characters.

b) For character sequence used as seeds for MD5 encryption, the length should be less than 16 characters.

6.2.4.4 FIA_SOS.2 TSF Generation of secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **the conditions defined in FIA_SOS.1**

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **OSPF and BGP**

6.2.4.5 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.

6.2.4.6 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 all the functions to the authorized identified roles who can be defined.

6.2.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.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 **administrator-defined roles**.

6.2.5.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 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.

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 policy
b) ACL policy
c) user management
d) definition of Managed Object Groups and 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

6.2.5.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **administrator-defined roles**.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from ***disclosure, modification*** when it is transmitted between separate parts of the TOE.

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 (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.

6.2.7.2 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the controlled resource:**bandwidth** 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**

6.2.8.2 FTA_TAB.1 Default TOE access banners

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

6.2.8.3 FTA_TSE.1 TOE session establishment

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

a) authentication

b) cut off command

c) 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***.

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 ***initial user authentication***

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	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

FPT_STM.1	O.Audit
FCS_COP.1	O.Communication O.Authentication
FCS_CKM.1	O.Communication
FCS_CKM.4	O.Communication
FDP_ACC.1	O.Authorization O.Forwarding
FDP_ACF.1	O.Authorization O.Forwarding
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication
FIA_SOS.2	O.Authentication
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Audit O.Authentication O.Authorization O.Forwarding
FMT_MOF.1	O.Authorization
FMT_MSA.1	O.Authorization
FMT_MSA.3	O.Authorization
FMT_SMF.1	O.Audit O.Authentication O.Authorization O.Communication
FMT_SMR.1	O.Authorization
FPT_ITT.1	O.Communication
FRU_PRS.1	O.Resource
FRU_RSA.1	O.Resource
FTA_SSL.3	O.Authentication
FTA_TAB.1	O.Authentication
FTA_TSE.1	O.Authentication O.Authorization
FTP_TRP.1	O.Communication O.Forwarding

Table 8: Mapping SFRs to 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), 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, which also require Cryptographic Support (FCS_COP.1). Cryptographic Support (FCS_COP.1) are also required where routing information exchange takes place.
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp (FPT_STM.1) 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 between TOE parts in FPT_ITT.1, and a trusted path for remote users in FTP_TRP.1. FCS_COP.1 addresses the 3DES/AES encryption of SSH channels. FCS_CKM.1 addresses keys generation of 3DES/AES/RSA. FCS_CKM.4 addresses key destruction of RSA. Note that keys of 3DES/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 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 password policy (FIA_SOS.1, FIA_SOS.2). Management functionality is provided in FMT_SMF.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), Warning of Non-Authorization access is provided in FTA_TAB.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 of Resource utilization is spelled out in FRU_PRS.1 and FRU_RSA.1

Table 9: SFR sufficiency analysis

6.3.3 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	FIA_UID.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
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_CKM.1	FCS_CKM.4	
FCS_CKM.4	FCS_CKM.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
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_SOS.2	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.1
FPT_ITT.1	None	
FRU_PRS.1	None	
FRU_RSA.1	None	
FTA_SSL.3	None	
FTA_TAB.1	None	
FTA_TSE.1	None	
FTP_TRP.1	None	

Table 10: Dependencies between TOE Security Functional Requirements

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components 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 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 via remote RADIUS server. This function is achieved by performing pass/fail action based on result from remote RADIUS authentication server.
3) Support authenticate user login using SSH, by password authentication, RSA authentication, or combination of both. 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 locking operation interface. This function is achieved by storing lock/unlock state in memory, and performing authentication when state is lock.
8) 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.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTA_TSE.1, FTA_SSL.3, FCS_CKM.4)

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.

(FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FTA_TAB.1,

FMT_MOF.1)

7.1.3 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 LPU in the TOE. If it is, the traffic will be sent to VRP in MPU for central process.

(FIA_UAU.2, FTP_TRP.1, FCS_COP.1, FIA_SOS.1, FIA_SOS.2, FCS_CKM.4)

7.1.4 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 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.

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

7.1.5 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. STelnet and SFTP are provided implementing secure Telnet and FTP, to substitute Telnet and FTP which are deemed to have known security issues.

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 as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1 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-TELNET. This function is achieved by providing implementation of Secure-TELNET.
7) Support Secure-FTP. This function is achieved by providing implementation of Secure-FTP.
8) Support periodic session key update. This function is achieved by periodically exchanging key information and storing them in memory.

(FCS_COP.1, FCS_CKM.1, FMT_SMF.1, FPT_ITT.1)

7.1.6 IP-based ACL

The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE to prevent internal traffic overload and service interruption.

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 ACL configurations into hardware.
3) Support rate limiting traffic based on screened traffic. This function is achieved by downloading configuration of rate into hardware.

(FMT_SMF.1, FRU_PRS.1, FRU_RSA.1)

7.1.7 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-Telnet/S-FTP;
6) Support configuration on service port for SSH;
7) Support configuration on authentication type, encryption algorithm for SSH;
8) Support authenticate user logged in using SSH, 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;

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, FTP_TRP.1)

7.1.8 Cryptographic functions

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

1) Support AES128/3DES/RSA algorithms. This is achieved by providing implementations of AES128/3DES/RSA algorithms.
2) Support MD5/HMAC-MD5 algorithms. This is achieved by providing implementations of MD5/HMAC-MD5 algorithms.

(FCS_COP.1)

7.1.9 Clock function

The MPU in TOE integrates clock module as the system clock source. It can provide the LPUs with 2.048 MHz synchronous clock signals.

The Clock function provides a reliable source of time for generation of timestamp in auditing functions.

Querying of time is also implemented by providing API on time-related functions.

1) Support configurations on attributes related to date and time, daylight saving hour, and time zone. This is achieved by providing interpreting input commands and storing result of interpreting in memory.
2) Support timing functions. This is achieved by reading clock signals generated by clock module, calculating difference of the readings and transforming the reading to human readable format.

(FMT_SMF.1, FPT_STM.1)

8 Abbreviations, Terminology and References

8.1 Abbreviations

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
LMT	Local Maintenance Terminal
RMT	Remote Maintenance Terminal
NE	NetEngine
CLI	Command Line Interface
GUI	Graphical User Interface
SRU	Switch Router Unit
MPU	Main Process Unit
LPU	Line Process Unit
SFU	Switching Fabric Unit
SPU	Service Process Unit

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.

Operator	See User.
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. July 2009. Version 3.1 Revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.