Huawei AR Series Service Routers V200R006C10 Security Target

Version: V1.4
Last Update: 2015-06-15
Author: Huawei Technologies Co., Ltd.

Revision record

Date	Revision Version	Change Description	Author
2014-04-25	0.1	Initial Draft	Yan Xiaojun
2014-10-11	0.2	Update TOE Identification	Sun Bin
2014-10-16	0.3	Update for the comments	Sun Bin
2014-11-14	0.4	Update for the review	Sun Bin
2014-11-25	0.5	Update for the review	Sun Bin
2014-11-29	0.6	Update for the review	Sun Bin
2015-01-08	0.7	Update for the information of AR series	Sun Bin
2015-03-13	0.8	Update the information about AR502	Sun Bin
2015-03-26	0.9	Update for the comments	Sun Bin
2015-03-27	1.0	Update for the comments	Sun Bin
2015-04-08	1.1	Update for the comments	Sun Bin
2015-04-23	1.2	Update for the comments	Sun Bin
2015-05-15	1.3	Update Physical scope	Sun Bin
2015-06-15	1.4	Update Physical scope	Sun Bin

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of Huawei AR Series Service Routers V200R006C10.

1.1 Security Target Identification

Name: Huawei AR Series Service Router V200R006C10 Security Target

Version: 1.3

Publication Date: 2015-05-15

Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei AR Series Service Routers

Version: V200R006C10SPC030

At the core of Huawei AR Series Service Routers is Versatile Routing Platform (VRP). Product software version V200R006C10 runs on VRP software Version 5 Release 16 with the following identifier (VRPV500R016C30), the software version of data plane is V200R006C10.

The naming examples of Huawei AR150/AR160/AR200 series are as follows:

Field	Meaning	Description
A	Product name	AR: application and access routers
B	Hardware platform type. The value can be 1 or 2.	• 1: four LAN interfaces • 2: eight LAN interfaces
C	Combines with B to indicate different router series using the same hardware platform.	The following router series are available: • 15: 4*FE LAN interface series • 16: 4*GE LAN interface series • 20: 8*FE LAN interface series
D	Type of major fixed uplink interfaces on the router	• 1: FE or GE • 2: SA • 6: ADSL-B/J • 7: ADSL-A/M • 8: G.SHDSL • 9: VDSL over POTS

Field	Meaning	Description
E	(Optional) Other interface types supported by the router	• E: enhanced major uplink interface (dual-uplink or two-wire/four-wire DSL enhanced) • F: uplink GE combo interface • G: uplink wireless interface (GPRS, 3G, or LTE) • V: voice interface • W: Wi-Fi interface
F	(Optional) Extended information about the router **NOTE** This field starts with "-" and specifies supplementary interface descriptions or other possible configurations.	• HSPA+7: WCDMA HSPA+7 3G standard • C: CDMA2000 3G standard • D: DC model • P: PoE supported • L: FDD-LTE, a European standard

Table 1: AR150/AR160/AR200 series routers naming conventions

The naming examples of Huawei AR510 series are as follows:

Field	Meaning	Description
A	Product name	AR: application and access routers
B	Hardware platform type	5: industrial integrated routing and switching platform
C	Combines with B to indicate different router series using the same hardware platform.	1: vehicle-mounted industrial router series
D	Type of major fixed uplink interfaces on the router	1: uplink GE electrical interface
E	(Optional) Other interface types supported by the router	• G: uplink wireless interface (LTE, 3G, or GPRS) • W: Wi-Fi interface
F	(Optional) Extended information about the router **NOTE** This field starts with "-" and specifies supplementary interface descriptions or other possible configurations.	• L: complies with FDD-LTE, a European standard. • A: supports audio input/output. • V (1 to n): supports video output. V2 indicates that the router supports two video outputs. (n is an Arabic number.)

Field	Meaning	Description
		• Mn: supports multiple-service open platform. (n is an Arabic number indicating the specifications of the multiple-service open platform. The larger the number, the larger capability the platform has. The M3 series is available now.)

Table 2: AR510/AR530/AR550 series routers naming conventions

The naming examples of Huawei AR530/AR550 series are as follows:

Example: AR531-F2C-H
AR531G-U-D-H

Field	Meaning	Description
A	Product name	AR: application and access routers
B	The hardware platform type	5: industrial integrated routing and switching platform
C	Combined with field B to represent a product series using a specific hardware platform	0: access IoT(Internet of Things) gateway 3: industrial switching router towards routing 5: industrial switching router towards switching
D	The type of major uplink interfaces on the device	1: FE/GE interface 2: LTE uplink
E	Type of auxiliary interfaces on the device (optional)	The value can contain zero or multiple letters. Meanings of these letters are: • G: wireless uplink interface (2G/3G) • Pe: HiSilicon or spread frequency shift keying (S-FSK) PLC • R: ZigBee or sub-GHz interface
F	Supplementary information about	• F: The six FE interfaces on the device are optical interfaces. If

T	interfaces (optional) **NOTE** This field contains zero, one, or multiple sub-fields that provide supplementary information or configurations of interfaces on the device. Multiple sub-fields are separated by hyphens (-).	the product name does not contain this field, the six FE interfaces are electrical interfaces. **NOTE** This value is fixed as F for the device providing optical interfaces. • nC: The device provides n combo interfaces. (n is an Arabic number.) • U: WCDMA 3G standard • L: FDD-LTE
G	Power supply information (optional)	• D: product model using DC power supply • Blank: product model using AC power supply (default)
H	Device type (optional)	H: industrial device

T
able 3: AR530/AR550 series routers naming conventions

The naming examples of Huawei AR1200/AR2200/AR3200 series are as follows:

Field	Meaning	Description
A	Product name	AR: application and access routers
B	Hardware platform series code	Currently, three router series are available: 1, 2 and 3. A larger value indicates higher performance.
C	Hardware platform type	2: traditional router 5: industrial router 6: Open Platform router
D	Maximum number of slots supported by the router	• AR1200 series: D indicates the maximum number of SIC slots supported. • AR2200 /AR3200 series: D indicates the maximum number of

• S I C : S		XISC slots supported. **NOTE** D can be 0, indicating the cost-effective router model with fixed uplink interfaces or reduced number of slots. E represents the number of fixed uplink interfaces or reduced number of slots.
E S m a	Fixed uplink interfaces on the router	• 1: FE/GE • 2: E1/SA • 4: four SIC slots **NOTE** If E is 0, the device has no fixed uplink interface.
F	(Optional) Other interface types supported by the router	• F: FE LAN interface • L: simplified interface • V: fixed voice interface • W: fixed Wi-Fi interface
G	(Optional) Extended information about the router **NOTE** This field starts with "-" and specifies supplementary interface descriptions or other possible configurations.	• A: AC model (AC is the default configuration, and this field can be omitted in AC models.) • D: DC model • 48FE: 48 fixed 100M switching ports

Table 4: AR1200/AR2200/AR3200 series routers naming conventions

- SIC: Smart Interface Card. This is the smallest card supported by ARs.
- WSIC: Wide SIC. The same height as a SIC, but twice the width.
- XSIC: Extended SIC. Twice the height and width of a SIC.
- EXSIC: Extra-Extended SIC. Twice the height of a SIC, and four times the width of a SIC

The TOE scope has been limited in terms of evaluated configurations by choosing the most relevant configurations of each series as can be found in the table below.

For each series, the minimum number of models has been selected in order to cover all the functionality that shall be tested as required by CC. The non evaluated models don’t provide extra functionalities that could interfere with the security.

The following table shows the evaluated configurations of each series.

Series	Device Name
AR150	AR151
	AR151G-C
	AR151G-HSPA+7
	AR151W-P

	AR156
	AR156W
	AR157
	AR157G-HSPA+7
	AR157VW
	AR157W
	AR158E
	AR158EVW
Ar160	AR161FG-L
	AR161FGW-L
	AR162F
	AR168F
	AR169BF
	AR169F
	AR169FGVW-L
	AR169FVW
	AR161FW-P-M5
	AR161
	AR161G-L
	AR169G-L
	AR169-P-M9
AR200	AR201
	AR201VW-P
	AR206
	AR207
	AR207G-HSPA+7
	AR207V-P
	AR207V
	AR207VW
	AR208E
AR1200	AR1220V
	AR1220W
	AR1220VW
	AR1220F
	AR1220E
	AR1220EV
	AR1220EVW
AR2200	AR 2220
	AR2204
	AR2240
	AR2201-48FE
	AR2202-48FE
	AR2220E
AR3200	AR3260
AR510	AR511GW-LAV2M3
	AR511GW-LM7
	AR513W-V3M8
AR502	AR502G-L-D
	AR502GR-L-D
AR530	AR531G-U-D
	AR531GR-U

	AR531GPE-U
	AR531-2C-H
	AR531-F2C-H
AR550	AR550-8FE-D-H
	AR550-24FE-D-H

Table 5: The device list of Huawei AR Series Service Routers

Sponsor: Huawei
Developer: Huawei
Certification ID:
Keywords: Huawei, VRP, Versatile Routing Platform, Access Routers

1.3 Target of Evaluation (TOE) Overview

Huawei AR Series Routers (AR200&AR1200&AR2200&AR3200) are the next-generation routing and gateway devices, which provide the routing, switching, wireless, voice, and security functions. Huawei AR provides a highly secure and reliable platform for scalable multiservice integration at enterprise and commercial branch offices of all sizes and small-to-medium sized businesses. It consists of both hardware and software.

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

MPU (Main Processing Unit) or 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 AR Series Service Routers V200R006C10 from a physical architectural view and a software architectural view.

The TOE is Huawei AR Series Service Routers (AR200&AR1200&AR2200&AR3200) 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 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 AR Series Service Routers use the multi-core CPU processing capabilities, Control and management plane and data forwarding plane are in the one board; but Core 0 is dedicated for control and management process, the other cores for

forwarding and services processes. In the software architectural, VRP uses VP (Virtual Path) to connect control plane and data forwarding plane.

1.4.1.1 Physical Architecture

1.4.1.1.1 Physical Architecture of Huawei AR Series Routers

When the TOE-enabled router 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, packet are forwarded through the internetworking device and forwarded to their configured destination. Routing protocols used are OSPF, and BGP.

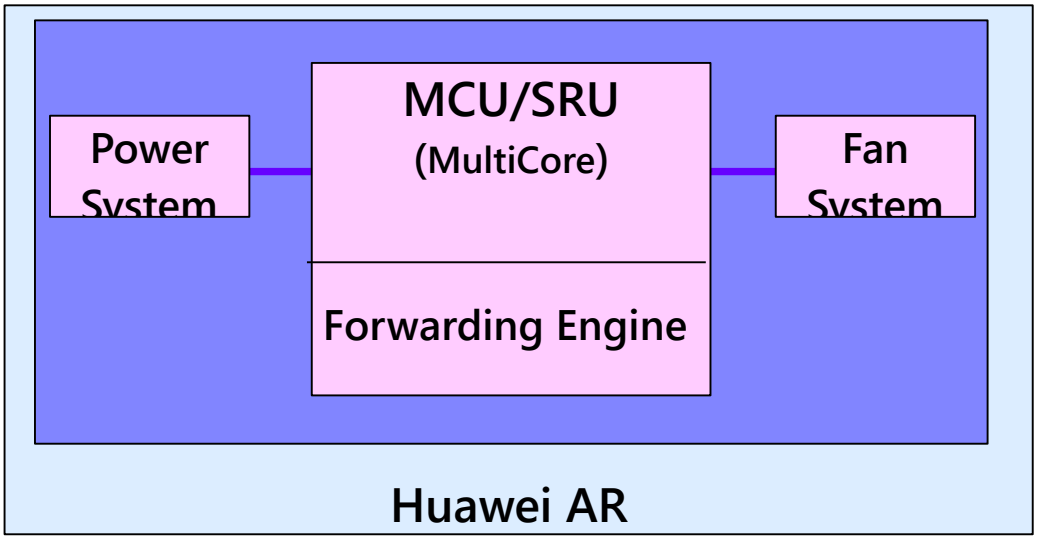

Figure 1: TOE Physical architecture of Framed AR

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

- Power system
- Fan system
- MCU/SRU
- Forwarding Engine

Except the network management system (NMS), all the other systems are in the integrated cabinet. The power system of AR 2240 and AR 3260, USR20 works in 1+1 backup mode. The functional host system (SRU/MCU) is the target of this evaluation and following introductions will focus on the functional host system only. The Network management system, power system, fan system, and switch fabric are not within the scope of this evaluation.

The functional host system is composed of the system backplane and SRUs/MCUs, SRU/MCU are the boards hosting the VRP which provides control and management functionalities. SRU/MCU also embeds a clock module as a source of system time. SRU/MCU is the board containing the forwarding engine and responsible 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 MCU 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**: Device lists which support 1+1 backup power (others only support one power): AR 2240,AR3260,*

1.4.1.2 Software Architecture

1.4.1.2.1 Software Architecture of AR

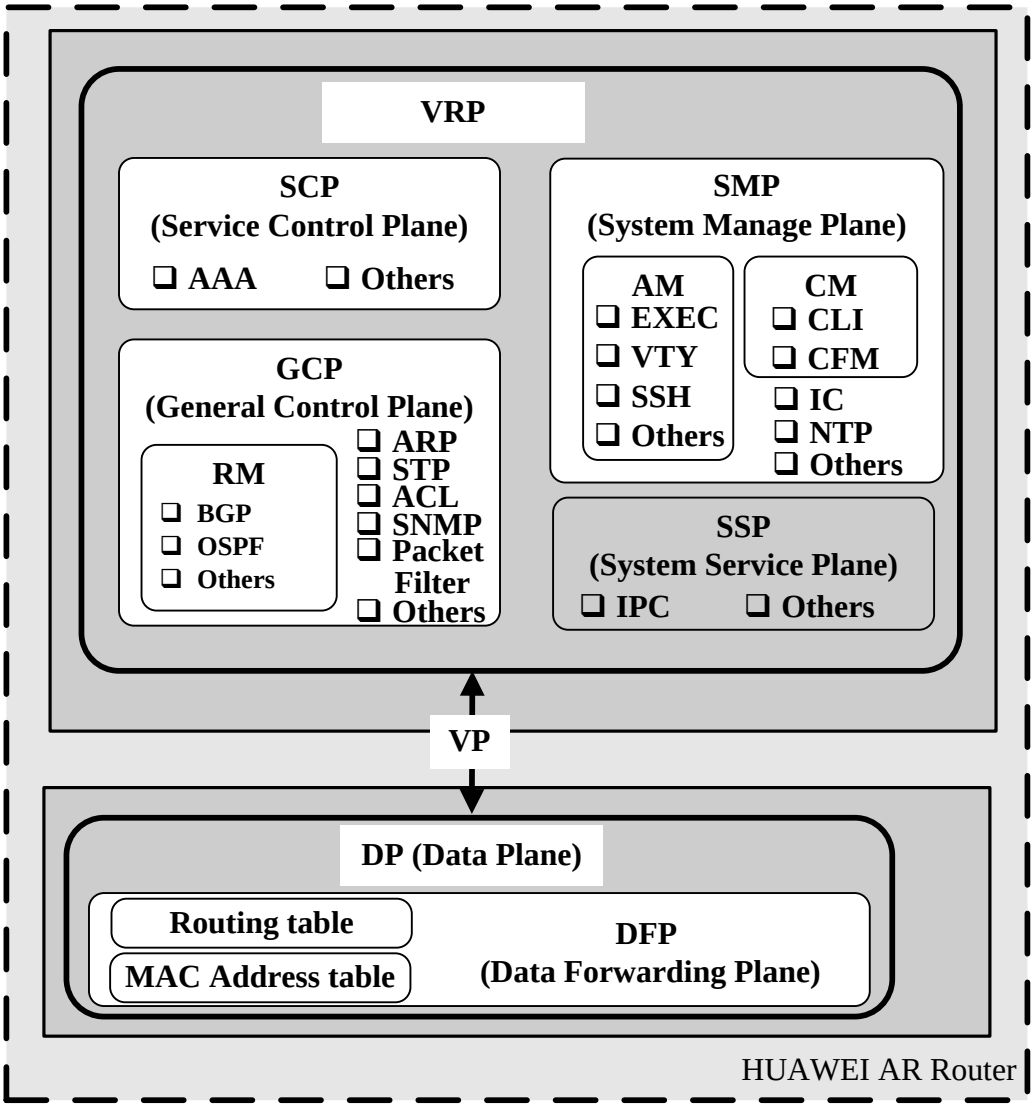

Figure 2: TOE Software architecture of AR

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

- Data plane
- Control and management plane
- Monitoring plane

Note that the **monitoring plane** is to monitor the system environment by detecting the voltage, controlling power-on and power-off of the system, and monitoring the temperature and controlling the fan. The monitoring plane is not considered 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 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/MCU. The VRP supports IPv4, 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 SRU(s). The VRP includes Service Control Plane (SCP), System Manage Plane (SMP), General Control Plane (GCP) and other TSF, non-TSF sub-systems.

1.4.2 Scope of Evaluation

This section will define the scope of the Huawei AR V200R006C10 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:

<table>
<tr><th>Model Types</th><th colspan="3">Typical System Configuration and Physical Parameters</th></tr>
<tr><td rowspan="10">AR1200
include(
AR1220V
AR1220W
AR1220VW
AR1220F
AR1220E
AR1220EV
AR1220EVW)</td><td>Item</td><td>Typical Configuration</td><td>Remark</td></tr>
<tr><td>Processing unit</td><td>AR1220F: 1GHz 2 Core
Others: 500MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512M</td><td>-</td></tr>
<tr><td>Flash</td><td>AR1220F:512M
Others: 256M</td><td>-</td></tr>
<tr><td>SD card</td><td>0</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>AR 1220F:1Mpps
Others: 450K PPS</td><td></td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>8FE + 2GE</td></tr>
<tr><td>SIC Slot</td><td>2</td><td></td></tr>
<tr><td>WSIC Slot</td><td>0</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>AR2200</td><td>Item</td><td>Typical Configuration</td><td>Remark</td></tr>
</table>

Include(AR2220 AR2201-48FE AR2202-48FE AR2204 AR2220E)	Processing unit	AR2201-48FE: 2-core 533 MHz AR2202-48FE: 2-core 533 MHz AR2204: 2-core 800 MHz AR2220: 4-core 600 MHz	-
	SDRAM	AR2201-48FE: 512 MB AR2202-48FE: 512 MB AR2204: 1 GB AR2220: 2 GB	-
	Flash	AR 2220: 16M Others: 512M	-
	SD card	AR 2220: 2GB Others: 0GB	MAX: AR2220: 4G Others : 2G
	Forwarding Performance	AR2201-48FE: 350 kpps AR2202-48FE: 350 kpps AR2204: 450 kpps AR2220: 1 Mpps	
	Fixed interface	GE	AR2201-48FE: 2GE+48FE AR2202-48FE: 2GE+48FE Others:3GE
	SIC Slot	4	
	WSIC Slot	2	
AR2240	**Item**	**Typical Configuration**	**Remark**
	Processing unit	600MHz 8 Core	-SRU40 main control board
	SDRAM	2G	-
	Flash	16M	-
	SD card	2 GB	MAX:4G
	Forwarding Performance	3M PPS	
	Fixed interface	GE	3GE WAN
	SIC Slot	4	
	WSIC Slot	2	
	XSIC Slot	2	
AR3260	**Item**	**Typical Configuration**	**Remark**
	Processing unit	750MHz 12 Core	-SRU80 main

<table>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td>control board</td></tr>
<tr><td>SDRAM</td><td>2G</td><td>-</td></tr>
<tr><td>Flash</td><td>16M</td><td>-</td></tr>
<tr><td>SD card</td><td>2 GB</td><td>MAX:4G</td></tr>
<tr><td>Forwarding Performance</td><td>5M PPS</td><td></td></tr>
<tr><td>Fixed interface</td><td>GE</td><td>3GE WAN</td></tr>
<tr><td>SIC Slot</td><td>4</td><td></td></tr>
<tr><td>WSIC Slot</td><td>2</td><td></td></tr>
<tr><td>XSIC Slot</td><td>4</td><td></td></tr>
</table>
</td></tr>
<tr><td>AR150
Include(
AR151
AR151G-C
AR151G-HSPA+7
AR151W-P
AR156
AR156W
AR157
AR157G-HSPA+7
AR157VW
AR157W
AR158E
AR158EVW
)</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>300K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>AR151:
4FE+1FE
AR151W-P:
4FE+1FE
AR151G-HSPA+7:
4FE+1FE
AR151G-C:
4FE+1FE
Others
:4FE</td></tr>
</table>
</td></tr>
<tr><td>AR160
Include(
AR161FG-L
AR161FGW-L
AR162F
AR168F
AR169BF
AR169F
AR169FGVW-L
AR169FVW
AR161FW-P-M5
AR161
AR161G-L
AR169G-L</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>AR169FVW: 1G
AR169FGVW-L: 1G
Others: 512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>350K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>5GE</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>AR169-P-M9）</td><td></td></tr>
<tr><td>AR200
Include(
AR201
AR201VW-P
AR206
AR207
AR207G-HSPA+7
AR207V-P
AR207V
AR207VW
AR208E）</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>450K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>8FE+1GE</td></tr>
</table>
</td></tr>
<tr><td>AR510
Include(
AR511GW-LAV2M3
AR511GW-LM7
AR513W-V3M8
)</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>1.2GHz 4Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>2GB</td><td>-</td></tr>
<tr><td>NAND Flash</td><td>2GB</td><td></td></tr>
<tr><td>EMMC FLASH</td><td>32GB</td><td></td></tr>
<tr><td>SD card</td><td>0 MB</td><td></td></tr>
<tr><td>Forwarding Performance</td><td>50K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>2GE</td></tr>
</table>
</td></tr>
<tr><td>AR502
Include(
AR502R-L-D
AR502GR-L-D
)</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>600MHz 2Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>128M</td><td>-</td></tr>
<tr><td>NAND Flash</td><td>512M</td><td></td></tr>
<tr><td>SD card</td><td>0 MB</td><td></td></tr>
<tr><td>Forwarding Performance</td><td>50K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>1GE</td></tr>
</table>
</td></tr>
<tr><td>AR530
Include(
AR531G-U-D
AR531GR-U
AR531GPE-U
AR531-2C-H</td><td>
<table>
<tr><th>Item</th><th>Typical Configuration</th><th></th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
</table>
</td></tr>
</table>

AR531-F2C-H)	Forwarding Performance	350K PPS	-
	Fixed interface	FE/GE	AR531-2C-H: 8FE+2GE AR531-F2C-H: 8FE+2GE Others: 6FE+2GE
AR550 Include(AR550-8FE-D AR550-24FE-D)	**Item**	**Typical Configuration**	**Remark**
	Processing unit	533MHz 2 Core	-
	SDRAM	512MB	-
	Flash	128MB	-
	SD card	0 MB	-not supported
	Forwarding Performance	450K PPS	-
	Fixed interface	FE/GE	AR550-8FE-H: 4GE+8FE AR550-24FE-H: 4GE+24FE

Table 6: Model Specifications

Table 3 details all physical interfaces available in TOE along with respective usage:

Boards	Supported Interfaces and Usage
MCU/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 "***AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description 16.pdf***". • SD card interface, SD memory card is the generic terms for any memory card or device built to SD standards, is used to hold a SD card to store data files as a massive storage device. The SD 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 SD 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. • 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. • 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.
SIC/WSIC/XSIC Interface Card	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 "***AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description 16.pdf***". • 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. • 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. The following interfaces if available according to hardware specification, will be disabled during 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. • E1/T1 interface, connector type E1/T1, supporting full-duplex, used for receiving and transmitting network traffic. • SA interface, Synchronous serial interface can function as a DCE or DTE, support multiple physical layer protocols, such as V.24, V.35, and X.21, and provide a maximum transmission rate of 2.048 Mbit/s. • ADSL interface:The ADSL-A/M and ADSL-B each provide 1-channel ADSL/ADSL2+ access, provide independent CPU and management interfaces, and support ADSL2+ Annex A, Annex B, and Annex M. 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 7: AR Interfaces Specifications

Type	Name	Version
Software	Product software	V200R006C10
	VRP	V500R016C30
	Linux	WRlinux4.3(AR150/AR160/AR200/AR530/AR550/AR1200/AR2200/AR3200) ANDROID4.1.2(AR510) WRLinux 4.3 with Linux kernel 3.4.5(AR502)
Guidance	AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description	Issue 16 / 2014-09-15
	AR V200R006C10 Product Manual	V1.0
	Common Criteria Security Evaluation – Certification Configuration	Version:1.4 / 2015-04-23

Table 8: List of software and guidance

1.4.2.2 Logical scope

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

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

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

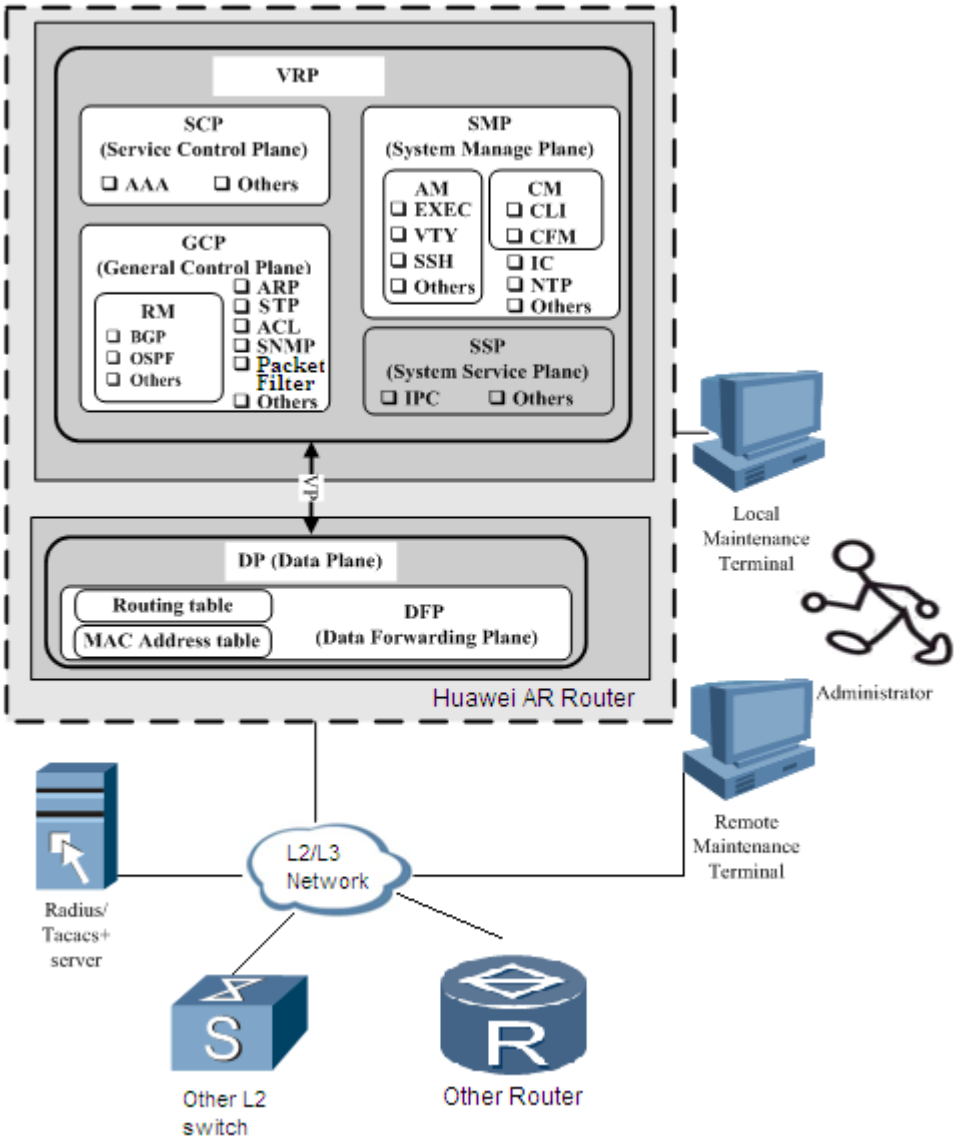

Figure 3: TOE logical scope

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.

TOE can be classified into Layer 2 forwarding and Layer 3 forwarding based on traffic forwarding.

When working as Layer 2 forwarding devices, the forwarding engine of TOE will forward the traffic according to MAC address. The MAC table entry will be automatically created by forwarding engine when Layer 2 forwarding.

When 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). 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 via a secure channel enforcing SSH.

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

- For management via the console, authentication is always enabled. Authentication mode is password. Length of password is no less than 8 characters
- 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 connections is supported. SSH server compatibility with version number less than 1.99 is considered a weakness, therefore to be disabled.

The environment for TOE comprises the following components:

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

1.4.3 Summary of Security Features

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 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	ping, tracert, quit,

User level	Level name	Purpose	Commands for access
		establishment of remote connections.	display
1	Monitoring	System maintenance	Level 0 and display, refresh, terminal, send
2	Configuration	Service configuration.	Level 0, 1 and all configuration commands.
3~15	Management	System management (file system, user management, internal parameters, fault diagnosis…).	All commands.

Table 9: Access Levels

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

By default, a user can log in to the device through the console port from the local host, and can use the commands at level 15 after authenticated successfully.

1.4.3.3 L2 Traffic Forwarding

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

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

Notes: AR502/AR510 Series don’t support L2 Forwarding.

1.4.3.4 L3 Traffic Forwarding

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

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

Notes:AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S don’t support BGP function. AR502G-L-D/AR502GR-L-D don’t support OSPF/BGP function.

1.4.3.5 Auditing

VRP generates audit records for security-relevant management actions and stores the audit records in memory or SD card 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 are 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.

1.4.3.6 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.

1.4.3.7 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 for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against ACL rules specified. Source MAC address, Destination MAC address, Ethernet protocol type, Source IP address, destination IP address, IP protocol number, source port number if TCP/UDP protocol, destination port number if TCP/UDP protocol, TCP flag if TCP protocol, type and code if ICMP protocol, fragment flag etc, can be used for ACL rule configuration

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

Notes: AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S don't support BGP function. AR502G-L-D/AR502GR-L-D don't support BGP/OSPF Function.

1.4.3.9 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 OSPF,SSH;
5) MD5 is used as verification algorithm for packets of BGP protocols from peer network devices;

1.4.3.10 SNMP Trap

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

A trap is a type of message used to report an alert or important event about a managed device to the NM Station.

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

1.4.3.11 STP

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

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

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

Notes: AR502G-L-D/AR502GR-L-D don't support STP.

1.4.3.12 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.

2 CC Conformance Claim

This ST is CC *Part 1 conformant [CC]*, *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC], *no extended.* The CC version of [CC] is 3.1R3.

No conformance to a Protection Profile is claimed.

No conformance rationale to a Protection Profile is claimed.

The TOE claims EAL3+ augmented with ALC_FLR.2.

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 route user who is able to send network traffic to the TOE that the TOE is not supposed to process.
- Unauthenticated Access A user who is not an administrator of the TOE gains access to the TOE management interface.
- 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.UnwantedL2NetworkTraffic Unwanted L2 network traffic sent to the TOE will cause the MAC table gets updated dynamically by MAC learning function . This may due 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 Unwanted L3 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 the Control Plane.

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 an administrator of the TOE gains access to the TOE management interface.

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.

3.1.2 Threats Components

- **T.UnwantedL2NetworkTraffic**
  - **Threat agent:** Route user.
  - **Asset:** TOE availability
  - **Adverse action:** Disturbance on TOE operation

- **T.UnwantedL3NetworkTraffic**
  - **Threat agent:** Route user.
  - **Asset:** TOE availability.
  - **Adverse action:** Disturbance on TOE operation.

- **T.UnauthenticatedAccess**
  - **Threat agent:** User who is not an administrator of the TOE.
  - **Asset:** TOE integrity and availability, user data confidentiality.
  - **Adverse action:** access to the TOE management interface.

- **T.UnauthorizedAccess**
  - **Threat agent:** An unauthorized personnel: attacker or authenticated user without privileges.
  - **Asset:** TOE integrity and availability, user data confidentiality.
  - **Adverse action:** perform unauthorized actions and unauthorized access to TOE information and user data.

- **T.Eavesdrop**
  - **Threat agent**: An eavesdropper (remote attacker) in the management network.
  - **Asset:** TOE integrity and availability, user data confidentiality and L3 network traffic.
  - **Adverse action:** 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 SD 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 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 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 in the TOE are accessible.

3.2.1.4 Authorized Administrators

A.NoEvil The authorized administrators are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

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. And TOE can find the loops in the network, and block certain interfaces to eliminate loops. 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.
- **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 Radius servers for obtaining authentication and authorization decisions.
- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console, and SD card inserted in the Router) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the management 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 for trustworthiness 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.UnwantedL3NetworkTraffic
O.Filter	T.UnwantedL2NetworkTraffic T.UnwantedL3NetworkTraffic

Table 10: 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
OE.Person	A.NoEvil

Table 11: 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. STP implementation assures an optimum forwarding path, preventing network from infinite loops, which can cause serious problems in the forwarding system and network efficiency. (O.Forwarding) ACL or Packet filter can deny unwanted L2 network traffic enter or pass TOE. (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 (O.Resource). ACL or Packet filter can deny unwanted L3 network traffic enter or pass TOE. (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).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSHv2 for communication between LMT/RMT and the TOE and SNMPv3 for communication between the TOE and the SNMP Trap Server. (O.Communication).

Table 12: 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.
A.NoEvil	The assumption that the personnel is not careless, willfully negligent, or hostile is addressed in OE.Person.

Table 13: 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)**, **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 the size of store device.**

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 CBC Mode** and cryptographic key sizes **128bits, 256bits** that meet the following: **FIPS 197**

6.2.2.2 FCS_COP.1/3DES Cryptographic operation

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

6.2.2.3 FCS_COP.1/RSA Cryptographic operation

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

6.2.2.4 FCS_COP.1/MD5 Cryptographic operation

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

6.2.2.5 FCS_COP.1/HMAC-MD5 Cryptographic operation

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

6.2.2.6 FCS_COP.1/DHKeyExchange Cryptographic operation

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

6.2.2.7 FCS_CKM.1/AES Cryptographic key generation

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

6.2.2.8 FCS_CKM.1/3DES Cryptographic key generation

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

6.2.2.9 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 (512bits-2048bits)** that meet the following: **RSA Cryptography Standard (PKCS#1)**

6.2.2.10 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 keygen method **DH Group Generation** and specified cryptographic key sizes **1024bits to 8192 bits** that meet the following: **RFC4419**

6.2.2.11 FCS_CKM.1/HMAC_MD5 Cryptographic key generation

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

6.2.2.12 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:

0. **user level**

b) commands and their following security attributes:

0. **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 or

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

6.2.3.3a FDP_DAU.1 Basic Data Authentication(for all series except AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S/AR502G-L-D/AR502GR-L-D)

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

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

6.2.3.3b FDP_DAU.1 Basic Data Authentication(for AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S)

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 OSPF, SSH, SNMP**

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

6.2.3.3c FDP_DAU.1 Basic Data Authentication(for AR502G-L-D/AR502GR-L-D)

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 SSH, SNMP**

FDP_DAU.1.2 The TSF shall provide **SSH, 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**.

6.2.3.5a FDP_IFF.1 Simple security attributes (for all series except AR502G-L-D/AR502GR-L-D/AR511GW-LAV2M3/AR511GW-LM7/AR513W-V3M8)

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 as source IP address, source 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, Ethernet protocol, VLAN-ID**.

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**.

6.2.3.5b FDP_IFF.1 Simple security attributes (for AR502G-L-D/AR502GR-L-D/AR511GW-LAV2M3/AR511GW-LM7/AR513W-V3M8)

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 as source IP address, source 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 **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.**

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/a (**for all series except AR502G-L-D/AR502GR-L-D**)The TSF shall provide a mechanism to verify that secrets meet **for text string used as seeds for MD5/HMAC-MD5 authentication for OSPF, they are case sensitive and contain no whitespace, no question mark. A cipher text mode should be used and the length of text string should be 16 to 392 characters.**

FIA_SOS.1.1/b (**for all series except AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S /AR502G-L-D/AR502GR-L-D**)The TSF shall provide a mechanism to verify that secrets meet **for password used as seeds for MD5 authentication for BGP, they are case sensitive and contain no whitespace, no question mark. A cipher password mode should be used and the length of password should be 16 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 MD5 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 16 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 MD5 authentication for SSH and they are case sensitive. A cipher password mode should be used and the length of password should be at least 8 characters long.**

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 all the functions** to the **administrator-defined roles**

6.2.5.2 FMT_MSA.1 Management of security attributes

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

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

6.2.5.3 FMT_MSA.3 Static attribute initialization

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

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

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

6.2.5.4 FMT_SMF.1 Specification of Management Functions

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

a) authentication, authorization, encryption 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
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**.

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable time stamps

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

6.2.6.1 FPT_FLS.1 Fail secure

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **packets to enter in an infinite loop**.

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 packet rate) to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to **controlled resources** (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 controlled resource: packet rate**, MAC address table entries** that ***subjects*** can use ***simultaneously***

6.2.7.3 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 (**for all series except AR502G-L-D/AR502GR-L-D/AR511GW-LAV2M3/ AR511GW-LM7/AR513W-V3M8)**The TSF shall ensure the operation of **Spanning Tree Protocol (STP) to cut off the loops** when the following failures occur**: packets to enter in an infinite loop .**

6.2.8 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_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***.

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
FDP_DAU.1	O.Authentication O.Forwarding
FDP_IFC.1	O.Filter
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

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
FMT_SMR.1	O.Authorization
FRU_PRS.1	O.Resource
FRU_RSA.1	O.Resource
FTA_SSL.3	O.Authentication
FTA_TSE.1	O.Authentication O.Authorization
FTP_TRP.1 FRU_FLT.1	O.Communication O.Forwarding O.Forwarding
FPT_FLS.1	O.Forwarding

Table 14: 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, FDP_DAU.1), 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. In order to prevent packets to enter in an infinite loop, provoking slow performance to network (FRU_FLT.1, FPT_FLS.1) STP is implemented.

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 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, 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 password policy (FIA_SOS.1). 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), 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 15: 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	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
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/AES Cryptographic key generation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary.[1]
FCS_COP.1/3DES Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/3DES Cryptographic key generation The key remains in the memory

[1] The key is SSH session key. After the session ends the key has no use, so no security issues if the key is not actively destructed.

		after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary.1
FCS_COP.1/RSA Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/RSA Cryptographic key generation FCS_CKM.4/RSA Cryptographic key destruction
FCS_COP.1/HMAC-MD5 Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/HMAC_MD5 Cryptographic key generation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary. 1
FCS_COP.1/MD5	FCS_CKM.1 FCS_CKM.4	No key for Md5, so the dependencies are unnecessary.
FCS_COP.1/DHKeyExchange Cryptographic operation	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DHKey Cryptographic key generation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary. 1
FCS_CKM.1/AES Cryptographic key generation	FCS_COP.1 FCS_CKM.4	FCS_COP.1/AES Cryptographic operation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary. 1
FCS_CKM.1/3DES Cryptographic key generationFCS_CKM.1	FCS_COP.1 FCS_CKM.4	FCS_COP.1/3DES Cryptographic operation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary. 1
FCS_CKM.1/RSA Cryptographic key generationFCS_CKM.1	FCS_COP.1 FCS_CKM.4	FCS_COP.1/RSA Cryptographic operationFCS_CKM.4 FCS_CKM.4/RSA Cryptographic key destruction
FCS_CKM.1/DHKey Cryptographic key generation	FCS_COP.1 FCS_CKM.4	FCS_COP.1/DH KeyExchange Cryptographic operation The key remains in the memory after use until it is overwritten by other data, so dependency of FCS_CKM.4 is not necessary. 1
FCS_CKM.1/HMAC_MD5 Cryptographic key	FCS_COP.1 FCS_CKM.4	FCS_COP.1/HMAC-MD5 Cryptographic operation

generation		
FCS_CKM.4/RSA Cryptographic key destruction	FCS_CKM.1	FCS_CKM.1/RSA Cryptographic key generation
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_DAU.1	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
FRU_PRS.1	None	
FRU_RSA.1	None	
FTA_SSL.3	None	
FTA_TSE.1	None	
FTP_TRP.1	None	
FPT_STM.1	None	
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FPT_FLS.1	None	

Table 16: 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 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 3 augmented with ALC_FLR.2, has been chosen to 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.
9) 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.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTA_TSE.1, FTA_SSL.3, FCS_CKM.1,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. This limitation of access also prevents users from accessing or deleting log files if they have insufficient rights.

(FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_MOF.1, FAU_STG.1)

7.1.3 L2 Traffic Forwarding

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

1) Support traffic isolation with VLANs
2) Support MAC address learning automatically
3) Support Layer 2 traffic forwarding based on MAC table entry
4) Support to configure MAC address statically
5) Support to configure black hole MAC address statically
6) Support to 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.

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

Notes: AR502/AR510 Series don’t support Layer 2 forwarding.

7.1.4 L3 Traffic Forwarding

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

1) Support ARP/ 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 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 MCU for central process.

(FIA_UAU.2, FTP_TRP.1, FCS_COP.1, FIA_SOS.1, FDP_DAU.1)

Notes: AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S don't support BGP protocol. AR502G-L-D/AR502GR-L-D don't support BGP/OSPF protocol.

7.1.5 Auditing

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

1) Support classification based on severity level. This function is achieved where logging messages are encoded with severity level and output to log buffer.
2) Support enabling, disabling log output. This function is achieved by interpreting enable/disable commands and storing results in memory. Log output is performed based on this result.
3) Support redirecting logs to various output channels: monitor, log buffer, trap

buffer, log file. This function is achieved by interpreting commands and storing results in memory or in log files in SD 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.
8) Support to automatically remove oldest log files if audit files exceed the size of store device.

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

7.1.6 Communication Security

The TOE provides communication security by implementing SSH protocol. Two versions of SSH: SSHv1 (SSH1.5) and SSHv2 (SSH2.0) are implemented. But SSH2 is recommended for most cases by providing more secure and effectiveness in terms of functionality and performance. 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 for RSA key destruction, overwriting it with 0

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

7.1.8 Security Management

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

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

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

Detailed function specification include following:

1) Support Local configuration through console port. Parameters include console port baud rate, data bit, parity, etc;
2) Support configuration for authentication and authorization on user logging in via console port;
3) Support configuration for authentication mode and authorization mode on user logging in via console port;

4) Support remotely managing the TOE using SSH.
5) Support enabling, disabling S-Telnet/S-FTP;
6) Support configuration on service port for SSH;
7) Support configuration on RSA key for SSH;
8) Support configuration on authentication type, encryption algorithm for SSH;
9) Support authenticate user logged in using SSH, by password authentication, RSA authentication, or combination of both;
10) Support configuration on logout when no operation is performed on the user session within a given interval;
11) Support configuration on max attempts due to authentication failure within certain period of time;
12) Support configuration on limiting access by IP address;
13) Support configuration on commands' access level;
14) Support management on OSPF by enabling, disabling OSPF;
15) Support configuration on area, IP address range, authentication type of OSPF;
16) Support management on BGP by enabling, disabling BGP;
17) Support configuration on peer address, authentication type of BGP;
18) Support management on ARP by specifying static ARP entry, aging time and frequency of dynamical ARP entry. This function is achieved by interpreting commands input and storing value in memory.
19) Support management on log by enabling, disabling log output;
20) Support configuration on log output channel, output host;
21) Support configuration ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
22) Support enabling, disabling SNMP Agent and Trap message sending function;
23) Support enabling, disabling the switch to Send an Alarm Message of a Specified Feature to the NM Station ;
24) Support setting the Source Interface, Queue Length and Lifetime of Trap message(*);
25) Support enabling, disabling STP function .
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, FTP_TRP.1)

7.1.9 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.
3) Support for RSA key destruction overwriting it with 0.

(FCS_COP.1, FCS_CKM.4)

7.1.10 Time

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

(FPT_STM.1, FTA_SSL.3)

7.1.11 SNMP Trap

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

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

(FDP_DAU.1)

7.1.12 STP

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

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

(FRU_FLT.1, FPT_FLS.1)

Notes: AR502/AR510 Series don’t support STP.

7.1.13 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 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
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
STP	Spanning-Tree Protocol
ACL	Access Control List
SNMP	Simple Network Management Protocol

8.2 Terminology

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

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

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

8.3 References

[ANSI 9.31] NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 using the 3-Key Triple DES and AES Algorithms, January 31, 2005

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012, Version 3.1 Revision 4, CCMB-2012-09-001, -002, -003

[CEM] Common Methodology for Information Technology Security Evaluation. Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004.

[FIPS 197] Federal Information Processing Standards Publication 197, November 26, 2001

[FIPS PUB46-3] Federal Information Processing Standards Publication 46-3, reaffirmed October 25, 1999

[PKCS#1 V1.5] PKCS#1 V1.5: RSA Encryption Standard, RSA Laboratories, Version 1.5, November 1993

[PKCS#1 V2.2] PKCS#1 V2.2: RSA Cryptography Standard, RSA Laboratories, Version 2.2, October 27, 2012

[RFC 1321] Request for Comments 1321, The MD5 Message-Digest Algorithm, April 1992

[RFC 2104] Request for Comments 2104, HMAC: Keyed-Hashing for Message Authentication, Feburary 1997

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

[RFC 4419] Request for Comments 4419, Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, March 2006

AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description 16.pdf