Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, Security Target Lite

Version: V3.7

Last Update: 2016-10-21

Author: Huawei Technologies Co., Ltd.

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of the Huawei AR Series Service Router AR1220 software, consisting of Versatile Routing Platform (VRP, V200R006C10), Concurrence Accelerate Platform (CAP) and the underlying OS. The TOE version is provided in chap. 1.2. The software is part of the Service Router AR1220, sometimes also referred to as AR1220 AC model.

1.1 Security Target Identification

Name: Huawei AR Series Service Router AR1220 software, consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, Security Target Lite
Identifier: AR1220_STL
Version: 3.7
Publication Date: 2016-10-21
Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei AR Series Service Router AR1220 software, consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS
Version: V200R006C10SPC030

The TOE is a software TOE consisting of Huawei's Versatile Routing Platform supported by the Concurrence Accelerate Platform and the underlying OS as described in the following chapters. The main purpose of the TOE is Layer 3 routing of incoming IP traffic. For details refer to chap. 1.4.2.
The identifier for the MPU hardware revision used for testing of the software TOE is AR01SRU1B VER.C.

Name: Huawei AR Series Service Router AR1220 software V200R006C10SPC030 - Preparative Procedures
Identifier: AR1220_PRE (Identifier comprises AR1220_PRE_PROD and AR1220_PRE_USER, see below)
<u>This document consists of two parts:</u>

1.) Name: Huawei AR Series Service Router AR1220 software V200R006C10SPC030 - Preparative Procedures for Production
Identifier: AR1220_PRE_PROD
Version: 1.1
SHA-2Hash:
e7cdf2ab785c7bd0be28dd2f003dd5cd764cd784e9031f4e1f337cb3668dbb5c
Remark: This document will be delivered only to facilities producing the TOE but to no other users.

2.) Name: Huawei AR Series Service Router AR1220 software V200R006C10SPC030 - Preparative Procedures for Users
Identifier: AR1220_PRE_USER

Version: 1.2
SHA-2Hash:
d3bb9dd9154b8fcc00ebd808518f12d36fd4fba5c7ecc28ad309f025a906505c

Name: Huawei AR Series Service Router AR1220 software - Operational User Guidance
Identifier: AR1220_OPE
Version: 1.1
SHA-2Hash:
7d3a8c8f2a6b76c16bac671518b0a3b6a4089fa7d9ef2981335643b977cce3b2

Name: Huawei AR Series Service Routers – Configuration and Reference
Identifier: AR1220_CR
Version: 1.1
SHA-2Hash:
c850e54d0a60896b7cf5b17fcfbcf75d9990a85c5bffb65290f8a36c28cfd6a6

For secure acceptance of the TOE parts that consist of documentation, the user needs to verify the SHA-2 Hash values provided in this document.
Sponsor: Huawei Technologies Co., Ltd.
Developer: Huawei Technologies Co., Ltd.
Certification ID: BSI-DSZ-CC-0992
Keywords: Huawei, VRP, Versatile Routing Platform, Access Routers, AR1220, AR1220 AC

1.3 General product overview

Huawei AR Series Routers 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) software deployed on MPU (Main Processing 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 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.

The following figure shows the front side of the AR1220. '1' denotes USB connectors for USB mass storage devices for external storage of audit information. '2' denotes the reset switch for the device.

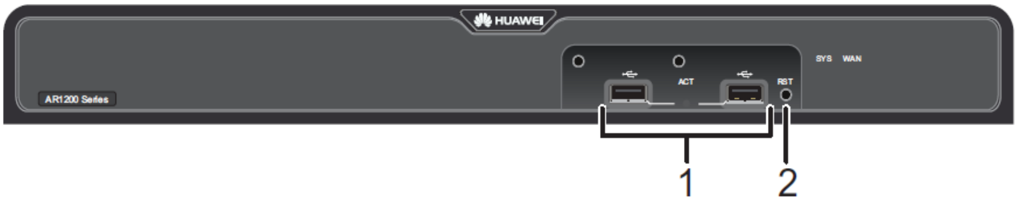


Figure 1: Front side of AR1220.

The following figure shows the back plane of the device. ‘1’ and ‘2’ denote connectors for the console (CON interface/MiniUSB interface), ‘3’ denotes two fixed GE electrical interfaces (i.e. GBit/s Ethernet connectors), ‘4’ denotes eight fixed FE electrical interfaces (i.e. 100MBit/s Ethernet connectors), ‘5’ denotes the power switch, ‘6’ denotes the power jack, ‘7’ denotes a jack reserved for a power cable locking latch, ‘8’ allows to attach physical locks, ‘9’ denotes the ESD jack, ‘10’ denotes two SIC slots for expansion cards, ‘11’ reflects the product model (i.e. AR1220), ‘12’ denotes an electrical ground point. There are no connectors to the AR1220 on the left side, right side, bottom or top of the device.

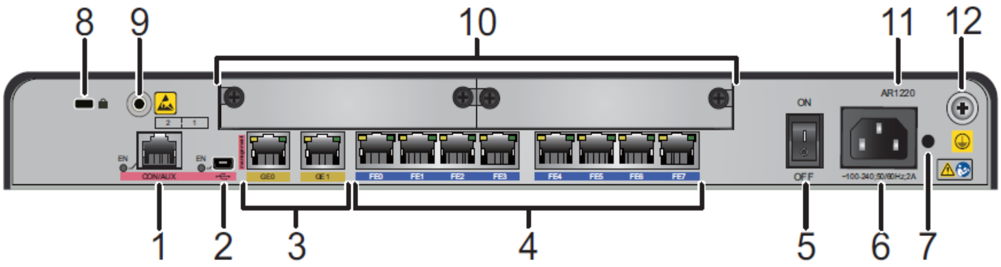


Figure 2: Back plane of AR1220.

1.4 TOE Description

This chapter provides an architectural overview of the AR1220 including a detailed description of the physical architecture and the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

1.4.1 Architectural overview of AR1220

This section will introduce the Huawei AR Series Service Router AR1220 from a physical architectural point of view and a software architectural point of view.

A router is a device that determines the next network point to which a packet should be forwarded towards its destination. It is located at any gateway (where one network meets another). A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGP, RIP, ISIS and OSPF. IP packets are forwarded to the router over one or more of its physical network interfaces, which process 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 AR1220 uses a dual-core CPU, Control and management plane and data forwarding plane are in one board. Core 0 of the CPU is dedicated to control and management process implemented by VRP, the other cores for forwarding and services processes like the Concurrence Accelerate Platform ('CAP') which will be explained later in this document.

1.4.1.1Physical Architecture of AR1220

When the router is attached to different networks on at least two of its network interfaces the router configuration determines how packet flows received on an interface will be handled. Typically, packets are forwarded through the internetworking device and forwarded to their configured destination. Routing protocols used are RIP, OSPF, ISIS, and BGP. The AR1220 provides one console port for connecting a local management terminal (LMT) and several Ethernet ports for connecting to networks (Remark: The back plane of AR1220 in figure 2 above actually shows two console ports – CON port and MiniUSB port. But only one of the two ports can be used at a time). These ports are part of the backplane of the device, additional ports can be added via expansion cards. In addition, two USB ports allow connection of mass storage devices to store audit data. Details about physical interfaces are provided in chapter 1.4.2.1.

For the management of the AR1220 an external network management system (NMS) can be used which is outside the actual router (i.e. outside the housing of the router) and not within the scope of this evaluation. The hardware of the AR1220 itself is not within the scope of this evaluation.

The functional host system is composed of the system backplane and SRU/MCU. SRU/MCU are the boards hosting the VRP and CAP which provide control and management functionalities. SRU/MCU also embeds a real time 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.

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 – functions which are not within the scope of this evaluation.

The general description about the hardware can be found in [AR Hardware Manual], chap. 2.7. The descriptions in [AR Hardware Manual] sometimes refer to the AR series as a whole or to the AR1200 series as a whole. The model representing the TOE is the 'AR1220' model, also referred to as 'AR1220 AC' model.

Information about the front panel and rear panel are provided in [AR Hardware Manual], chap. 2.7.2. Indicators are described in [AR Hardware Manual], chap. 2.7.3.

The details about the physical configuration of the TOE are summarized in the following table (see also [AR Hardware Manual], chap. 2.7.6).

Model Types	Typical System Configuration and Physical Parameters		
	Item	**Typical Configuration**	**Remark**
AR1220 (AR1200 series)	Processing unit	AR1220: 500MHz 2 Core	-
	SDRAM	512M	-
	Flash	AR1220: 256M	Internal NOR Flash
	SD card	0	-not supported

	Forwarding Performance	AR1220: 450K PPS	
	Fixed interface	Fast Ethernet (FE)/ Gigabit Ethernet (GE)	8FE + 2GE
	SIC Slot	2	
	WSIC Slot	0	The 2 SIC Slots can be used as 1 WSIC Slot.

Table 1: Model Specification

Table 2 details all physical interfaces available in TOE along with respective usage. Interfaces are also described in [AR Hardware Manual], chap. 2.7.4. Detailed information about interface cards can be found in [AR Hardware Manual], chap. 5.3.

Boards	Supported Interfaces and Usage
MCU/SRU	The following list shows a collection of interfaces. The description about indicators on panel can be found in user manual ***[AR Hardware Manual]***”. • GE 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 receiving and transmitting network traffic. Available ports: GE0, GE1 (backplane). • FE interface, connector type RJ45, operation mode 10M/100M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002, used for receiving and transmitting network traffic. Available Ports: FE0, FE1, …FE7 (backplane) • ETH interface used for connections initiated by users and/or administrators from a local maintenance terminal via SSH to perform management and maintenance operations. The ETH interface is not a separate physical interface but uses either one of the GE interfaces or one of the FE interfaces, which is up to configuration by the administrator. The default port for ETH upon delivery is the GE0 interface. • 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. Available ports: CON/AUX (backplane) • MiniUSB connector, connector type MiniUSB compatible with USB 2.0 for USB based consoles (backplane) • USB interface, connector type USB compatible with USB 2.0 standard used to hold a USB disk to store data files as a mass storage device. Available ports: 2 USB ports (front)

Table 2: AR Interfaces Specifications

The following figure provides a schematic overview of the basic flow of traffic.

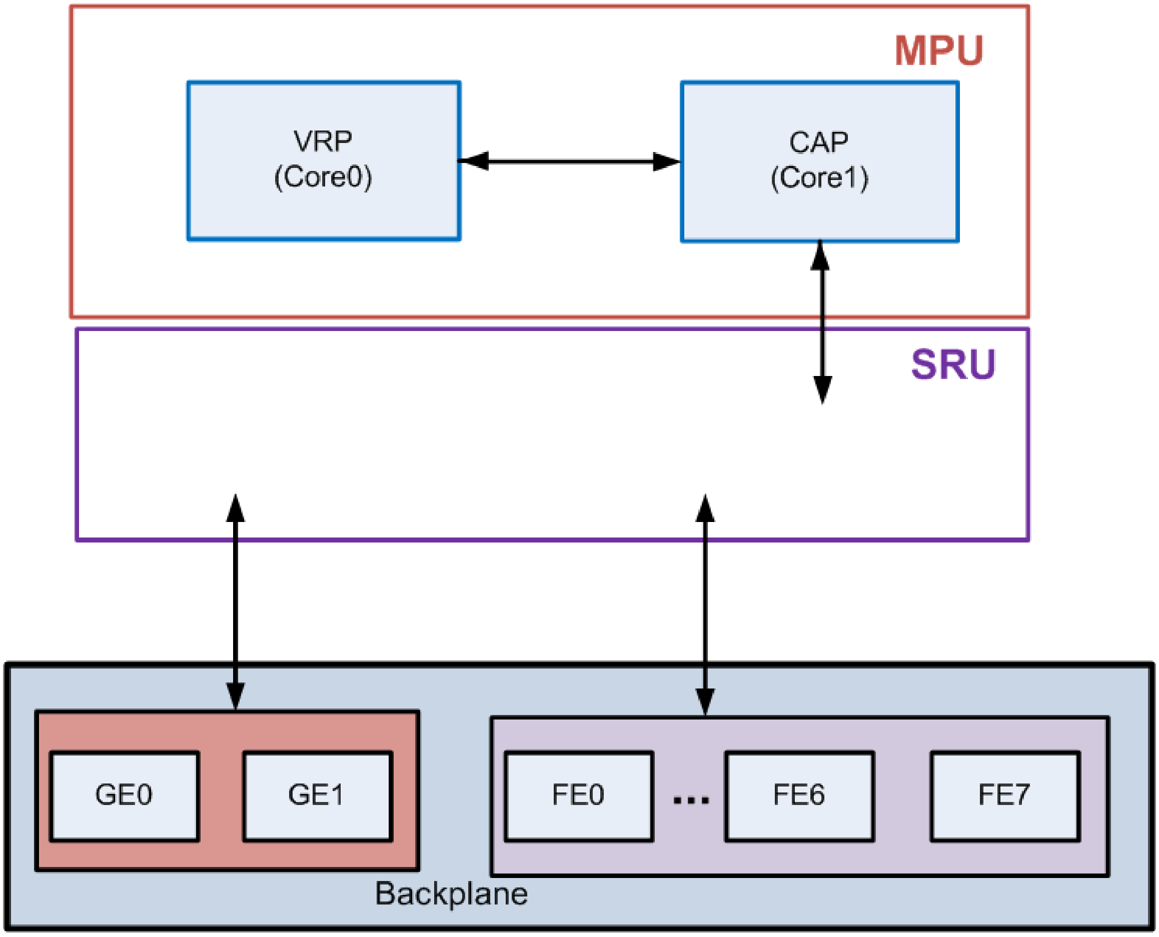


Figure 3: Physical Architecture of AR1220.

The connectors on the backplane are connected to the MPU through the SRU.
All L3 traffic that goes through the MPU goes through the Concurrence Accelerate Platform ('CAP') software first. CAP can either forward traffic directly (if the route is known to CAP) or sends it to the Versatile Routing Platform ('VRP') software first. In the latter case, VRP determines the route to the destination, sends the packet back to CAP and CAP forwards it to the intended destination. The route information is then also stored on the CAP for future use.
The CPU of the AR1220 is a dual core CPU. VRP software and CAP software are running on different cores of the CPU – VRP is running on Core0 and CAP is running on Core1.

The figure above contains Ethernet based ports (for RMTs) only, but omits the console port (for LMT). The LMT is connected to the MPU directly because the traffic from the console port is not filtered. See also the description in the following chapters.

Figure 3 is intended to demonstrate how the TOE (software, see next chapters) interacts with the underlying hardware.

1.4.1.2Software Architecture of AR1220

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

- Data plane
- Control and management plane

Note that from a product's point of view there is an additional plane – the so-called **monitoring plane**. This 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 is not part of the TOE and will therefore not be further covered.

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

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

The VRP is the control and management platform that runs on the SRU/MCU. The VRP supports IPv4/IPv6, and routing protocols such as RIP, Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), ISIS 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.

The AR1220 handles L2 and L3 traffic. Since L2 traffic is handled by the SRU itself without additional security related control or management functionality, only L3 forwarding capabilities are within the scope of this certification.

VRP is supported by the Concurrence Accelerate Platform (CAP) for performance reasons. VRP and CAP are relying on the underlying Windriver OS. The relation of VRP, CAP and the OS is described in more detail in chap. 1.4.2.3.

1.4.2 Scope of Evaluation

This section will define the scope of the part of the Huawei AR1220 comprising the TOE to be evaluated.

1.4.2.1Physical scope

The TOE is software only consisting of VRP, CAP and the underlying OS. This will be discussed in more detail in the next chapter. In addition, the evaluation documentation including the guidance documentation as well as the product manual is part of the TOE (for versions please refer to chap. 1.2).

1.4.2.2Logical scope

The logical boundary is represented by the elements that are displayed with a white background within the rectangle in the figure below. The TOE consists of VRP and

CAP software as well as the underlying OS (see white boxes in Figure 4). In addition, the related documentation belongs to the TOE but is omitted for the rest of this chapter. As shown in Figure 3, the MPU hosts the components VRP and CAP which run on different cores. The TOE is only running on the two cores of the CPU. The SRU contains third party products which do not contain TOE software. The MPU also hosts the OS which is not reflected by Figure 4. The TOE provides several security functions which are described in more detail in chap. 1.4.3.

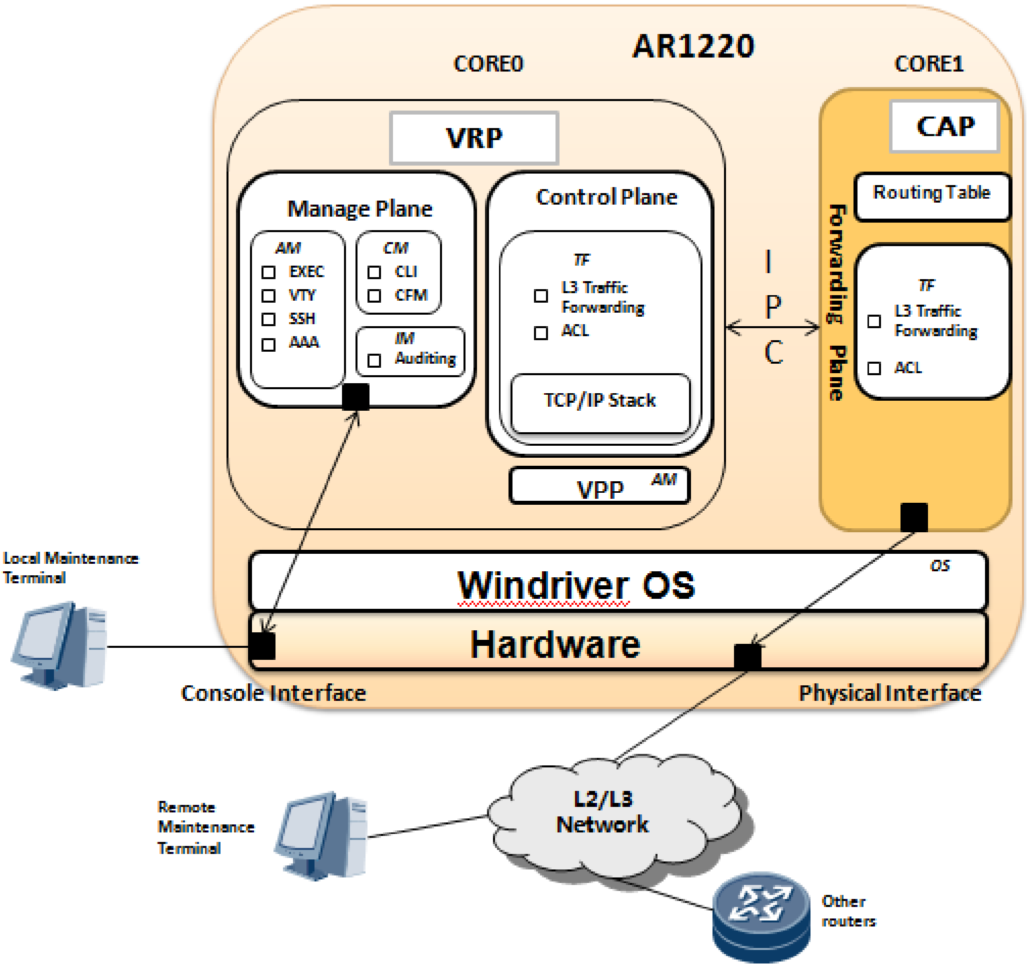


Figure 4: TOE logical scope.

Figure 4 reflects also the basic structure of the TOE with respect to subsystems. Abbreviations of the TOE's subsystems are formatted in *italic* with the following meaning: AM: Access Management, CM: Command Management, IM: Information Management, TF: Traffic Forwarding, OS: Operating System.

Although the AR1220 is capable of L2 and L3 forwarding only Layer 3 forwarding is regarded as TOE functionality. L2 forwarding is handled by the third party switches outside the TOE scope independently from CAP and VRP. All routing decisions for L3 traffic are done by CAP and VRP.

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 of CAP.
System control and security management are performed either through LMT which is connected to the Management plane of the TOE directly via the Console interface (there is no traffic filtering performed for the traffic via the console port) or through RMT via a secure channel enforcing SSH via the ETH port on the backplane.

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 or Authentication, Authorization, Accounting (‘AAA’, i.e. username and password). Length of password is no less than 8 characters
- For management via the ETH interface, authentication is always enabled. Authentication mode is password or username and password (AAA). Length of password is no less than 8 characters
- Service of TELNET and FTP have to be disabled to use the TOE in the certified configuration.

The environment for TOE comprises the following components:

- Other switches and Routers used to connect the TOE for L2/L3 network forward.
- 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.

1.4.2.3Interaction between VRP, CAP and Windriver OS

The following figure shows the basic interaction between VRP, CAP and the underlying Windriver OS.

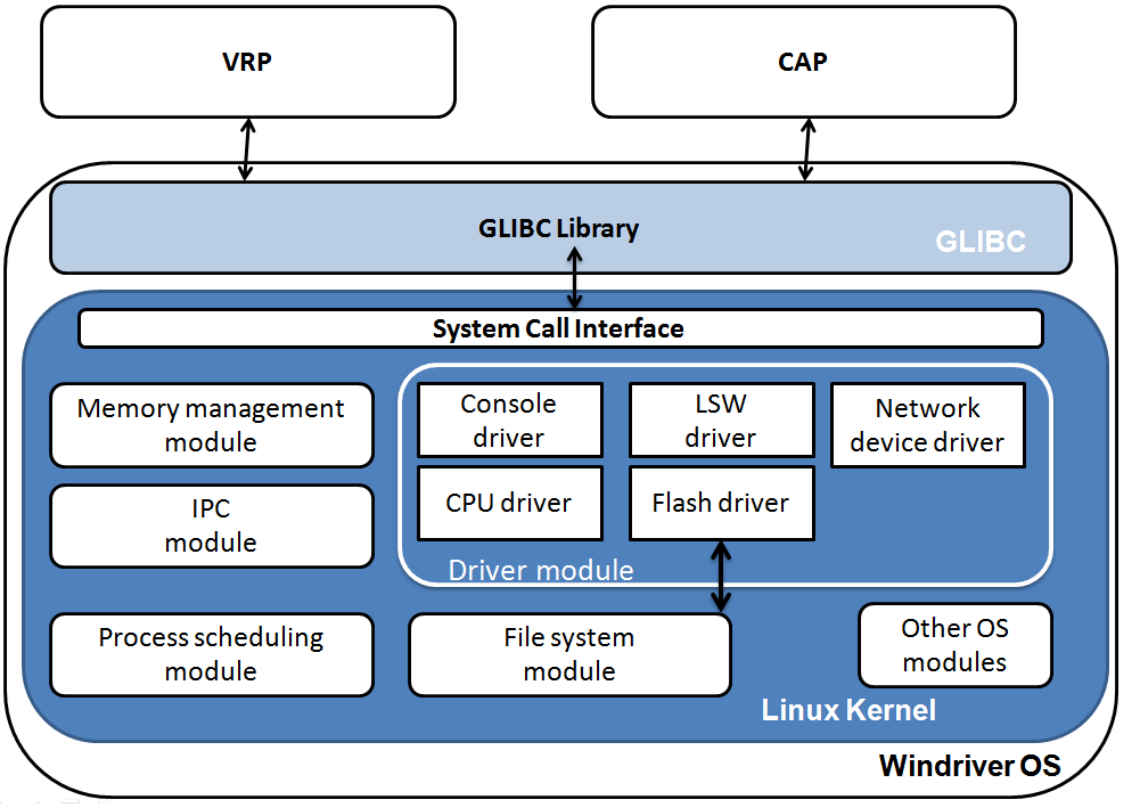


Figure 5: Interaction between VRP, CAP and Windriver OS

The interaction of VRP and CAP and the Linux Kernel modules is performed through the GLIBC library and the System Call Interface of the Linux Kernel. The Linux Kernel and the GLIBC Library are part of the Windriver OS.

Among others the following modules are part of the Linux kernel:

- Memory management module
- IPC module (Inter Process communication)
- Process scheduling module
- Filesystem module
- Driver module including:
  - Console driver
  - LSW driver
  - CPU driver
  - Flash driver
  - Network device driver

Both, VRP process and CAP process are started and maintained by the Process scheduling module of the Linux Kernel. VRP and CAP are depending on the Memory management module. For Inter Process Communication (IPC) between VRP and CAP, the IPC module of the Linux Kernel is called. For access to driver information, the driver module of the Linux kernel is used.

VRP will access the console file to read data from and write data to the console. VRP will access the configuration file for the LAN switches of the SRU to configure the LAN Switch (LSW) chip, etc. VRP writes the audit data in flash memory using the file system module of the Linux kernel.

1.4.3 Summary of Security Features

1.4.3.1Authentication

The TOE can be accessed either through LMT (i.e. the ‘console’) or RMT (i.e. via virtual terminals, ‘VTYs’). The TOE supports one console and up to 15 VTYs. For managing the LMT or RMT, the user needs sufficient user level according to the TOE’s Access Control (see chap. 1.4.3.2). For all types of terminals the user has to authenticate with username and password (AAA). After 3 consecutive failed authentication attempts the user account will be blocked for 5 minutes before the user can try to authenticate again.

Only authenticated users can execute commands of the TOE (except the ones for authentication which need to be executable also for non-authenticated subjects).The default user level for users is ‘0’. Only one user level can be assigned to a user account. So the user level of a user is unambiguous at any time. Upon the delivery of the TOE one user account with user level ‘15’ is present on the TOE. This account is intended to be used for set up and administration of the TOE.

The use of external Radius or TACACS+ servers for user authentication is not permitted for the certified use of the TOE.

User authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP) sessions. User authentication for access via the console is always enabled. The use of SSH connection is always required for accessing the TOE via RMT. For LMT no logically secured communication channel is required.

The TOE allows specifying minimum requirements on the length and complexity of passwords.

1.4.3.2Access Control

The TOE manages user privileges by access level. There are in total 16 hierarchical access levels ranging from 0 ~ 15. The bigger the number, the higher is the privilege. Correspondingly, levels from 0~15 can be assigned to all commands provided by the TOE. A user can access a command if the command’s access level is less or equal to the user’s access level. The default access level for the default administrator account is 15. By default, commands are registered with level 0 ~ 3.
The four default hierarchical access control levels are reflected by the following table.

User level	Level name	Intended Purpose	Commands for access
0	Visit	Network diagnosis and establishment of remote connections.	ping, tracert, language-mode, super, quit, display
1	Monitoring	System maintenance	Level 0 and display, debugging, reset, refresh, terminal, send
2	Configuration	Service configuration.	Level 0, 1 and all configuration

User level	Level name	Intended Purpose	Commands for access
			commands.
3	Management	System management (file system, user management, internal parameters, fault diagnosis …).	All commands.

Table 3: Default Access Levels

All authenticated users with an access level equal or higher to the access level of the command are allowed to execute the corresponding command. Users with lower access levels will not be able to execute the corresponding command.
In case there has been no user level associated with the user account, the default user level ‘0’ is used.
A user with sufficient user privileges (e.g. default administrator at level 15) can modify the default configuration and can register commands with different levels. A user cannot perform tasks, though, that would exceed his level. For example, a user at level 5 can change the command level of a command from e.g. 3 to 5 but not beyond 5, because this would be higher than his user level (for this example it is assumed that the command level of the command to modify command levels is not higher than 5, otherwise the user at user level 5 couldn’t execute the command at all).
A user can also not perform modifications to user accounts that are registered to a higher level than his own. For example a user of level 5 cannot modify a user account of level 15 even if he would have the necessary rights to execute the command for modification of user levels. This protects on the one hand higher level user accounts but also prevents users to increase their own user level. A user with sufficient access rights to execute the command to modify user levels can lower his user level, though (e.g. from 5 to 3).
The TOE can be accessed either through LMT (i.e. the ‘console’) or RMT (i.e. via virtual terminals, ‘VTYs’).

1.4.3.3L3 Traffic Forwarding

The TOE handles forwarding policy at its core. The forwarding engine controls the flow of network packets by making (and enforcing) a decision with regard to the network interface that a packet gets forwarded to.
ACLs define which traffic flow is allowed and which traffic flow is forbidden. ACLs can be defined on L3 level based on ARP (IP addresses, tcp/udp ports, protocols) (see chap. 1.4.3.6 for details).

1.4.3.4Auditing

VRP generates audit records for security-relevant management actions. All audit records contain not only the information on the event itself but also a timestamp and – where possible – additional information like user ID, source IP, etc.

Audit functionality is activated by default but can be deactivated by users with sufficient access rights. Logging of the event of disabling audit functionality is enforced by default.

Audit records are stored in the NVRAM when events are logged. From there, audit records can be either displayed on the terminal (local terminal or VTY), written to the internal NOR Flash, an external USB Mass Storage Device or an external audit server. Writing to an external audit server is independent from displaying, writing to NOR Flash or writing to USB Mass Storage Device. When an external USB Mass Storage Device is used, the internal NOR Flash cannot be used in parallel. Note: The internal NOR Flash is a hard-wired Flash Card and is therefore also sometimes referred to as ‘Flash Card’. This Flash Card cannot be removed or exchanged without disassembling the device and is therefore regarded as internal Flash memory.
The events are written to the NVRAM at first. Using NVRAM ensures that no audit data is lost in case of power loss. If the log information is exceeding 100kB, the oldest entries will be overwritten (cyclic overwriting).

If the device is configured to display log information on the terminal, any new log information is displayed immediately after the associated event occurred.

The content of the NVRAM can be written to the NOR Flash on demand but not automatically. If the storage space of the NOR Flash is used up, the system does not allow further storage of log events on the NOR Flash. The user has to free space on the NOR Flash first (e.g. by manually deleting older audit information from the file system).

If a USB Mass Storage Device is connected and configured as output device for audit information, audit information is automatically written to the USB Mass Storage Device when the log information is exceeding 100kB. The audit information in the NVRAM will be overwritten afterwards starting with the oldest entries (cyclic overwriting). Every time the log information is exceeding 100kB, the log information is written to the USB Mass Storage Device again. A different file name is used every time so the log information in the USB Mass Storage Device is not overwritten by new log files. Writing a log file to the USB Mass Storage Device can also be performed on demand by a user with sufficient access rights (e.g. in case an administrator wants to write the audit information from NVRAM to the USB storage device at a specific time). If a USB Mass Storage Device is attached to the AR and is configured as output device for audit information, audit information cannot be copied to the NOR Flash at the same time.

Writing to an external audit sever can either be done in plaintext (UDP) or protected by using SSL protocol. The scope of the certification is restricted to plaintext communication, so the TOE, the external audit server and the communication line between them have to be protected physically.
If the TOE is connected to an external audit server and set up to send audit information to it, audit information is sent from the NVRAM to the external audit server immediately after the associated event occurred.

1.4.3.5Communication Security

The TOE enforces communication security by implementing the SSH2 (SSH2.0) protocol for RMT.
To protect the TOE from eavesdrop and to ensure data transmission security and

confidentiality, SSH2 provides:

- Authentication of the TOE by means of RSA 2048bits, PKCS#1 V2.1, RSASSA-PKCS1-v1_5;
- Authentication of client by means of RSA 2048bits, PKCS#1 V2.1, RSASSA-PKCS1-v1_5 according to the 'publickey' method defined in [RFC 4252];
- 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.
Beside SSH (which is sometimes also referred to as ‘Secure Telnet’ or ‘STelnet’) SFTP is provided implementing secure FTP based on SSH as communication protocol.

1.4.3.6ACL

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 to the traffic before forwarding it into the remote network. Packet flows on Layer 3 arriving at a network interface of the TOE are checked to ensure that they conform with the configured packet filter policy. For this, the TOE offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces.
Users with sufficient access rights 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. 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, etc, can be used for ACL rule configuration.
Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is forwarded by default.

1.4.3.7Security 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 audit, as well as suppression of repeated log records

All security management functions (i.e. commands related to security management) require sufficient user level for execution (see description of access control for details, chap. 1.4.3.2).

1.4.3.8 Cryptographic functions

The security features of the TOE require some cryptographic functions. They are defined in chap. 7.1.7.

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC], extended by security functional components as defined in chap. 5, and *CC Part 3 conformant* [CC]. There are no extended components defined for CC Part 3*.* The CC version used is 3.1R4.
No conformance to a Protection Profile is claimed.
This ST is conforming to assurance package EAL2 without augmentations.

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 The TOE receives network traffic that the TOE is not supposed to process.
- Unauthenticated Access A subject that is not a user of the TOE gains local or remote access to the TOE for managing the device.
- 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 local management terminal or remote management terminal (LMT/RMT).

3.1.1 Threats

T.UnwantedL3NetworkTraffic Unwanted L3 network traffic sent to the TOE will not only cause the TOE's processing capacity for incoming network traffic to be consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when this traffic is sent to the Control Plane.

This may further cause the TOE to fail to respond to system control and security management operations.

T.UnauthenticatedAccess A subject that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data without permission.

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. By that he could modify TOE configuration data without permission.

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 which are not protected against modification and disclosure that are exchanged between TOE and LMT/RMT.

3.1.2 Threats Components

- T.UnwantedL3NetworkTraffic
  - Threat agent: A subject that is not a user of the TOE.
  - Asset: wanted L3 network traffic.

- Adverse action: The subject could send too much unwanted L3 network traffic to exhaust the resources of the TOE and by that compromising L3 forwarding capabilities of the TOE. As a result, wanted L3 network traffic could be dropped (TOE availability).

- T.UnauthenticatedAccess
  - Threat agent: A subject that is not a user of the TOE.
  - Asset: TOE configuration data
  - Adverse action: A subject that did not authenticate to the TOE gets access to the TOE and by that could be able to modify TOE configuration data without permission (compromising TOE integrity and availability).

- T.UnauthorizedAccess
  - Threat agent: Unauthorized personnel,: i.eauthenticated user with insufficient privileges.
  - Asset: TOE configuration data.
  - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to modify TOE configuration data without permission (compromising TOE integrity and availability).

- T.Eavesdrop
  - Threat agent: An eavesdropper (remote attacker) in the management network.
  - Asset: TOE configuration data, L3 network traffic.
  - Adverse action: Intercept, and potentially modify or re-use information from L3 network traffic which is exchanged between TOE and RMT. By this confidentiality and integrity of the data exchanged could be compromised (could affect confidentiality of user data and TOE integrity and availability).

3.2 Assumptions on the environment for the use of the TOE

A.PhysicalProtection It is assumed that the TOE (including any console attached, including any USB storage device attached) is protected against unauthorized physical access. The TOE is assumed not to contain any residual information that could be used for an attack when it is removed from the physically protected environment (e.g. for repair by a third party or at the end of life when the device is disposed).

A.NetworkElements The environment is supposed to 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. Examples of such devices are:

- AR1220 internal LAN Switches of the SRU for L2 and L3 switching
- Peer router(s) for the exchange of dynamic routing information;
- Remote entities (PCs) used for administration of the TOE.

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.

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

A.CorrectWorkingHardware
It is assumed that the underlying hardware of the AR1220, which is outside the scope of the TOE, works correctly. This includes the real time clock (RTC) of the hardware. The TOE produces time stamps based on the time information received from the RTC of the hardware.

A.UpToDateClient
It is assumed that the user uses a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

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 to a configured route for the destination IP address of the packet (L3 routing).
The TOE shall provide Access Control List (ACL) functionality that can be configured to drop unwanted L3 network traffic.

Remark: This objective focuses on the process of forwarding and does not require a guarantee of forwarding 100% of incoming data.

O.Communication The TOE must implement logical protection measures for network communication between the TOE and Remote Management Terminal (RMT) from the operational environment. These protection measures shall include device authentication and the use of a secure communication protocol.

O.Authorization The TOE shall implement different authorization levels that can be assigned to users in order to restrict the functionality that is available to individual users.

O.Authentication The TOE shall support the authentication of users by local username and password. This applies to local (Local Management Terminal, LMT) and remote access (Remote Management Terminal, RMT). The authentication mechanisms shall allow identifying users. This information shall also be provided to other security functions if required (e.g. user identities for audit functionality).

Remark: The use of RADIUS or TACACS+ servers for user authentication is not permitted for certified use of the TOE.

O.Audit The TOE shall provide functionality to generate audit records for security-relevant events.

O.SecurityManagement The TOE shall provide functionality to securely manage security functions provided by the TOE. This includes:

- Set-up and modification of ACL policy
- Definition and maintenance of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests
- Set-up and modification of authentication, authorization and encryption policies
- Management of user accounts and user data (including the assignment of user access levels)
- Definitions and maintenance of managed objects groups and command groups.

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, LAN Switches of the SRU for L2 and L3 switching, other routers for the exchange of routing information and PCs used for TOE administration.

OE.Physical The TOE (i.e., the complete system including attached peripherals, such as a console and USB mass storage devices) shall be protected against unauthorized physical access. Whenever the TOE is removed from the physically protected environment, it shall not contain any residual information that could be used for an attack.

OE.NetworkSegregation The ETH interface in the TOE shall 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.

OE.Person Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE. This includes instruction to follow and abide the instructions provided by the TOE documentation.

OE.CorrectWorkingHardware
The underlying hardware of the AR1220 shall work correctly. This includes the real time clock (RTC) of the hardware. The TOE produces time stamps based on the time information received from the RTC of the hardware.

OE.UpToDateClient
The user shall use a secure remote management terminal for remote administration of the TOE which is up to date with respect to supported cryptographic algorithms and security measures.

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. UnwantedL3NetworkTraffic
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess
O.Authorization	T.UnauthorizedAccess

O.Audit	T.UnauthenticatedAccess T.UnauthorizedAccess
O.SecurityManagement	T. UnwantedL3NetworkTraffic T.UnauthenticatedAccess T.UnauthorizedAccess T.Eavesdrop

Table 4: Mapping Objectives to Threats

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

Environmental Objective	Threat / Assumption
OE.NetworkElements	A.NetworkElements
OE.Physical	A.PhysicalProtection
OE.NetworkSegregation	A.NetworkSegregation
OE.Person	A.NoEvil
OE.CorrectWorkingHardware	A.CorrectWorkingHardware
OE.UpToDateClient	A.UpToDateClient

Table 5: Mapping Objectives for the Environment to Threats, Assumptions

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal of that threat:

Threat	Rationale for security objectives to remove Threats
T.UnwantedL3NetworkTraffic	The TOE performs L3 forwarding of network traffic. ACL functionality can be used to deny unwanted L3 network traffic to enter or pass the TOE. (O.Forwarding) ACL functionality can be configured by users with sufficient user level (O.SecurityManagement)
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). Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement). Detected attempts of unauthenticated access are regarded as security relevant events which lead to

	the generation of a related audit record (O.Audit).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). Access control mechanisms (including user levels and command levels) can be configured by users with sufficient user level (O.SecurityManagement). Detected attempts of unauthorized access are regarded as security relevant events which lead to the generation of a related audit record (O.Audit).
T.Eavesdrop	The threat of eavesdropping is countered by requiring communication security via SSHv2 for communication between RMT and the TOE (O.Communication). Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement).

Table 6: Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.NetworkElements	The assumption that the external environment provides securely and correctly working network devices such as peer router for routing information exchange, and management terminals for TOE control and management is addressed in OE.NetworkElements.
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access and that the TOE does not contain residual information that could be used for an attack whenever the TOE is removed from the physically protected environment is expressed by a corresponding requirement in OE.Physical.
A.NetworkSegregation	The assumption that the TOE is not accessible via the application (or public) networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation.
A.NoEvil	The assumption that the administrators of the TOE are not careless, willfully negligent, or hostile is addressed in OE.Person.
A.CorrectWorkingHardware	The assumption that the underlying hardware is working correctly is expressed by a corresponding

	requirement in OE.CorrectWorkingHardware.
A.UpToDateClient	The assumption that the user is using a remote management terminal which is up to date regarding cryptographic algorithms and security measures is expressed by a corresponding requirement in OE.UpToDateClient.

Table 7: Sufficiency analysis for assumptions

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:
    - o User identities.
    - o Locally managed passwords.
    - o Locally managed access levels.
- Audit configuration data.
- Audit records.
- Configuration data of security feature and functions
- Routing and other network forwarding-related tables, including Link layer address resolution tables.
- 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.

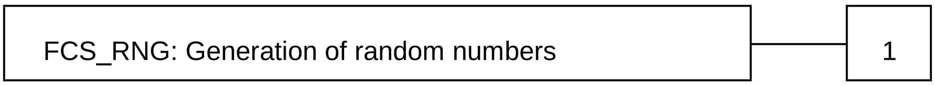
5 Extended Components Definition

There is one extended component defined which refers to random number generation and is taken from chap. 3.1 [AIS20].

5.1 FCS_RNG Generation of random numbers

Family Behaviour
This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:



FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1
There are no management activities foreseen.

Audit: FCS_RNG.1
There are no actions defined to be auditable.

FCS_RNG.1 Random number generation
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].
.

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/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

6.2 Definition of security policies

To avoid redundancy in the definition of SFRs, in this chapter the security policies are defined that have to be fulfilled by the TOE.

6.2.1 VRP access control policy

The access control policy is implemented through authentication and access control mechanisms as described in chap. 1.4.3.1 and 1.4.3.2 respectively.
The VRP access control policy defines the following subjects, objects and attributes:

Subjects:

- users

Objects:

- commands

Information security attributes:

- user level
- access level of command groups (i.e. ‘command level’)

6.2.2 VRP information control policy

The VRP information control policy defines the following subjects and attributes:

Subjects:

- network packets

Information security attributes:

- source IP address,
- destination IP address,
- transport protocol,
- source tcp or udp port number,
- destination tcp or udp port number.
- hardware interface used for SSH connections

Whenever an incoming network packet is intended to be forwarded, the VRP information control policy mandates to check the Access Control List (ACL) defined for VRP. The rules in ACL refer to handling of the network packet on layer 3.

Rules for layer 3 could either permit or deny forwarding based on the information security attributes ‘source IP address’, ‘destination IP address’, ‘transport protocol’, ‘source tcp or udp port number’, ‘destination tcp or udp port number’. Rules have to contain at least one of the attributes but may contain several attributes.

For every incoming network packet that is intended to be forwarded the ACL is checked for a rule that matches the attributes of the packet or frame, respectively starting from the first entry in the ACL. The ACL is checked until the first matching rule is found. The network packet is then either forwarded or discarded according to the matching rule in the ACL.

If no matching rule is found, the network packet is forwarded.

6.3 TOE Security Functional Requirements

6.3.1 Security Audit (FAU)

6.3.1.1FAU_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

ii. management of user accounts

1. add, delete, modify (including password reset and change of user level)

2. password change (by the user himself)

3. session termination

iii. management of command groups

1. add, delete, modify (including change of command levels)

iv. authentication policy modification

v. system management

1. reset to factory settings

2. operation requests (i.e. configuration of the device after start-up)

vi. log management

1. log policy modification

Application Note: Changes to user levels are covered by c.ii.1.modify. Changes to command levels are covered by c.iii.1.modify. Audit functionality shall be enabled by default during start-up of the device. The audit functionality cannot be shut down manually. The audit functionality can only be shut down by shutdown of the AR1220 itself. In that case there is only an audit record generated for the shutdown of the device but not the audit functionality in particular.

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).**

Application Note: The term 'if applicable' shall be read as 'whenever an event can be associated with the specified information'. For example if an event can be associated with a User ID, then the event shall be audited and the audit information shall contain the User ID. If the event cannot be associated with the User ID, the event shall be audited and the audit information shall not contain User ID information. If multiple conditional information can be associated with an event (e.g. interface and User ID can be associated with an event), all the conditional information shall be contained in the audit information when auditing the event.

6.3.1.2FAU_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.

6.3.1.3FAU_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.

6.3.1.4FAU_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.

6.3.1.5FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **forward the oldest audit data to the selected permanent storage location** if the audit trail exceeds **100kB**.

Application Note: At first all audit information is written to NVRAM (buffer). If the audit trail in the buffer exceeds 100kB, the audit information will be forwarded to the selected permanent storage location which can be the internal NOR Flash or external USB mass storage device (if present). In addition, audit data can be sent to external audit servers (if present). After the audit data has been forwarded from the

NVRAM buffer to the permanent storage location, the NVRAM buffer will be cleared and newly generated audit data will be written to the NVRAM buffer.

6.3.2 Cryptographic Support (FCS)

6.3.2.1FCS_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 operating in CTR mode** and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [FIPS SP 800-38A].**

Application Note: AES-128 in CTR mode is used for encryption and decryption within SSH communication.

6.3.2.2FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1 The TSF shall perform **asymmetric authentication** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048bits** that meet the following: **RSA Cryptography Standard ([PKCS#1 V2.1], RSASSA-PKCS1-v1_5 for SSH)**

Application Note: RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication of the TOE (server) to the client for SSH according to chap. 6.6 [RFC 4253], ssh-rsa as well as 'publickey' authentication of the client to the TOE(server) for SSH according to chap. 7 [RFC 4252].

6.3.2.3FCS_COP.1/HMAC-SHA1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **data integrity generation and verification** in accordance with **a specified cryptographic algorithm HMAC-SHA1** and cryptographic key sizes **160 bits** that meet the following: [**RFC 2104], [FIPS 198-1]**

Application Note: HMAC-SHA1 is used for integrity protection of SSH communication.

6.3.2.4FCS_COP.1/SHA256 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with **SHA256** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4]**

Application Note: SHA256 is used for hashing passwords before storage in non-volatile memory .

6.3.2.5FCS_CKM.1/DH Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **diffie-hellman-group14-sha1** and specified cryptographic key sizes **2048bits** that meet the following: [**RFC 4253], [RFC 3526], [PKCS#3] for SSH.**

Application Note: The TOE generates a shared secret value with the client during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption (AES-128-CTR) and generation and verification of integrity protection information (HMAC-SHA1) for SSH communication. The key generation is performed according to [RFC 4253], chap. 7.2.

6.3.2.6FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm keygen method **RSA** and specified cryptographic key sizes **2048bits** that meet the following: **[FIPS 186-4], chap. 5.1., RSA keypairs for RSASSA-PKCS1-V1_5 using CRT.**

6.3.2.7FCS_CKM.2/DH Cryptographic key distribution

FCS_CKM.2.1/DH The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **diffie-hellman-group14-sha1** that meets the following: **[RFC 4253], [RFC 3526], [PKCS#3] for SSH.**

6.3.2.8FCS_CKM.4/RSA Cryptographic key destruction

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

Application Note: This SFR was refined to RSA keys only. The destruction mechanism has to be triggered manually.

6.3.2.9FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1 The TSF shall provide a ***deterministic*** random number generator that implements:

- DRG.2.1: *If initialized with a random seed of 32 bytes that shall contain at least 100 bit entropy in each half of the value (16 most significant bytes and 16 least significant bytes) the internal state of the RNG shall have Min-entropy of at least 100 bits.*
- DRG.2.2: *The DRNG provides forward secrecy.*
- DRG.2.3: *The DRNG provides backward secrecy.*

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

- DRG.2.4: The RNG, initialized with a random seed of 256 bits during the preparative operations ensured by the preparative procedures for users generates output for which more than 2^{14} strings of bit length 128 are mutually different with probability greater than $1-2^{-8}$.
- DRG.2.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must

pass test procedure A **and no other test suites**.

Application Note: The operations have been performed according to chap. 4.7 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 100 bit entropy in each half of the value (16 most significant bytes and 16 least significant bytes) The seed value has to be provided by the user to the TOE before enabling SSH communication. The TOE verifies that the random seed has been set before activation of SSH is possible. If the random seed has not been provided by the user, the TOE will not allow activation of SSH communication. Since the output of the RNG is used only for SSH communication with respect to TSF, it is thereby ensured that the random seed is set before any TSF uses random numbers from the DRG.2 random number generator. It is recommended to use a seed value from a class PTG.2 PTRNG or equal or above quality to generate the seed value.

6.3.3 User Data Protection (FDP)

6.3.3.1FDP_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**.

6.3.3.2FDP_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:

i. **user level**

b) commands and their following security attributes:

i. **access level of command groups (i.e. ‘command level’)**

Application Note: For every command there is an associated access level which can be set by the administrator to a value between 0 and 15 (see chap. 1.4.2.3 for details as well as for default configuration upon delivery of the TOE). The term ‘command groups’ refers to commands on the same level.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
The user level of the user corresponds to or exceeds the access level of the Command Group he is accessing by trying to execute a command.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
None.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the
the
following additional rules:
None.

6.3.3.3FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the authentication information of SSH.**
.FDP_DAU.1.2 The TSF shall provide **SSH** with the ability to verify evidence of the validity of the indicated information.

6.3.3.4 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **VRP information control policy(based on ACL) as defined in chap. 6.2.2** on **the network traffic, the ACL-defined information, and rules defined in the ACL either permitting or denying forwarding of the network traffic based on Information Security attributes as defined in chap. 6.2.2.**

6.3.3.5 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the VRP **information control policy (based on ACL) as defined in chap. 6.2.2** based on the following types of subject and information security attributes:
Subjects:

- **network packets or frames,**

Information security attributes:

- **source IP address,**
- **destination IP address,**
- **transport protocol,**
- **source tcp or udp port number,**
- **destination tcp or udp port number,**
- **hardware interface used for SSH connections**

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(based on ACL) as defined in chap. 6.2.2, and the policy's action is permit**.

FDP_IFF.1.3 The TSF shall enforce the **VRP information control policy as defined in chap 6.2.2**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **None**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following
rules: **None**.

6.3.3.6 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource*** from the following objects: **Trusted Path**.

Application Note: Whenever a Trusted Path is terminated for whatever reason, all temporary session keys are erased from the volatile memory by the post-processing routines associated with the Trusted Path. These session keys are generated by FCS_CKM.1/DH and are used by FCS_COP.1/AES, and FCS_COP.1/HMAC-SHA1, respectively.

6.3.4 Identification and Authentication (FIA)

6.3.4.1FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***3*** **consecutive 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 and block the user account for authentication for at least 5 minutes**.

6.3.4.2FIA_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) SHA256 hashes of passwords

d) temporary blocking time for user accounts after unsuccessful authentication attempts

e) time when users are logging in and logging off.

6.3.4.3FIA_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.

Application Note: Authentication is possible by username and password._

6.3.4.4FIA_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.

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

6.3.5 Security Management (FMT)

6.3.5.1FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***modify the behavior, determine the behavior*** of the functions **identified in FMT_SMF.1** to **users with sufficient user level.**

Application Note: Access control of the TOE works as follows: User levels are assigned to all commands and all users. Users can only execute a command if their associated user level is equal or higher compared to the user level assigned to a command. The management of user levels also depends on this access control mechanism. According to the default access control level settings upon TOE delivery, all commands are registered between command levels 0 and 3. The default administrator account upon delivery is registered to level 15. Management of user levels and command levels is restricted to users of levels equal or higher to the level of the corresponding commands for administration. So the term 'administrator' is not so easy to define in general for the TOE, because a user might have a sufficient user level to execute some commands for TOE administration (or management) but not all of them and the associated user levels and command levels are subject to change. A user of user level 15, though, always has access to all commands. A user of certain user level cannot perform operations with a resulting state above his own user level. In particular, assuming he would have sufficient user level to perform changes to user level or command level in general, he can still not modify user accounts with a user level higher than his own and he cannot change a command level to a value beyond his user level.

6.3.5.2FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/ACFATD 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 **users with sufficient user level**.

Application Note: See Application Note for FMT_MOF.1 for clarification.

FMT_MSA.1.1/IFF The TSF shall enforce the **VRP access control policy** to restrict the ability to ***modify, delete*** the security attributes **identified in FDP_IFF.1** to **users with sufficient user level.**

6.3.5.3FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1/ACFATD The TSF shall enforce the **VRP access control policy** to provide ***permissive*** default values for security attributes (Command Group associations) that are used to enforce the SFP.
FMT_MSA.3.2/ACFATD The TSF shall allow **users with sufficient user level** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1/IFF 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/IFF The TSF shall allow **users with sufficient user level** to specify alternative initial values to override the default values when an object or information is created.

6.3.5.4FMT_SMF.1 Specification of Management Functions

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

a) **Define and maintain IP addresses and address ranges (via ACL policy) that will be accepted as source addresses for traffic forwarding (L3 forwarding). Define and maintain IP addresses and address ranges (via ACL policy) that will be accepted for remote administration (TOE administration)**
b) **Set-up of TOE accepted cipher suites**
c) **Configure the interval for user inactivity after that an established session is terminated**
d) **Configure the minimum time a user account is blocked after failed attempts for user authentication**
e) **Manage user accounts and user data**
f) **Define and maintain Command Groups**
g) **Configure audit functionality including output channel and output host for audit data.**
h) **Activate SSH functionality after seed has been provided to the deterministic random number generator.**
i) **Define hardware interface for remote administration.**

Application Note: Management of user levels is covered by option e), management of command access levels is covered by option f).

6.3.5.5FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **users with associated user levels**.
FMT_SMR.1.2 The TSF shall be able to associate users with roles.
Application Note: See Application Note for FMT_MOF.1 for clarification.

6.3.6 Protection of the TSF (FPT)

6.3.6.1FPT_STM.1 Reliable time stamps

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

Application Note: The reliable time stamps are based on the information of the real time clock (RTC) of the hardware. The RTC itself is not part of the TOE. The time stamps rely on the correct operation of the RTC of the underlying hardware as defined in OE.CorrectWorkingHardware.

6.3.7 TOE access (FTA)

6.3.7.1FTA_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 by a user with sufficient user level.**

Application Note: Termination of an interactive session results in the loss of user authentication. This mechanism applies to local connections via console as well as remote connections via RMT.

6.3.7.2FTA_TSE.1 TOE session establishment

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

a) user authentication failure
b) Source IP address (applies to remote administration only)
c) hardware interface for remote administration

6.3.8 Trusted Path/Channels (FTP)

6.3.8.1FTP_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***

Application Note: To establish a trusted path, the SSH protocol shall be used that complies with RFCs 4344 [RFC4344], 4251 [RFC 4251], 4252 [RFC 4252], 4253 [RFC 4253] and 4254 [RFC 4254]. For encryption the AES-128 algorithm (CTR mode) shall be used which is in agreement with [RFC 4344]. For Data Integrity, the HMAC-SHA1 algorithm shall be used which is in agreement with [RFC 4253]. For Key Exchange the diffie-hellman-group1-sha1 algorithm shall be used which is in agreement with [RFC 4253], [RFC4344]. For client authentication the TOE shall support 'publickey' authentication according to chap. 7 [RFC4252]. Server authentication is performed using RSA according to chap. 6.6 [RFC 4253], ssh-rsa. In addition, SFTP (i.e. FTP based on SSH protocol) is supported for secure file transfer. SSH communication is sometimes also referred to as ‘STelnet’.

6.4 Security Functional Requirements Rationale

6.4.1 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_STG.1	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/SHA256	O.Communication
FCS_CKM.1/DH,FCS_CKM.1/RSA	O.Communication
FCS_CKM.2/DH	O.Communication
FCS_CKM.4/RSA	O.Communication
FCS_RNG.1	O.Communication
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FDP_DAU.1	O.Communication
FDP_IFC.1	O.Forwarding
FDP_IFF.1	O.Forwarding
FDP_RIP.1	O.Communication
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Authentication O.Authorization
FMT_MOF.1	O.Authorization
FMT_MSA.1/ACFATD	O.Authorization
FMT_MSA.1/IFF	O.Forwarding
FMT_MSA.3/ACFATD	O.Authorization
FMT_MSA.3/IFF	O.Forwarding
FMT_SMF.1	O.SecurityManagement
FMT_SMR.1	O.Authorization
FPT_STM.1	O.Audit
FTA_SSL.3	O.Communication
FTA_TSE.1	O.Communication
FTP_TRP.1	O.Authentication O.Communication

Table 8: Mapping SFRs to objectives

6.4.2 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 requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF and FMT_SMF.1.

O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable. Requirements on reading audit records are defined in FAU_SAR.1. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the size of the log file becomes larger than 100kB in the NVRAM buffer, audit information is sent to the permanent storage location and the buffer is cleared afterwards as required by FAU_STG.3.
O.Communication	Communication security is implemented by the establishment of a trusted path for remote users in FTP_TRP.1. Requirements on the security of the device authentication to establish a secure communication channel are defined in FDP_DAU.1. FCS_COP.1 addresses the AES encryption of SSH channels. FCS_CKM.1/RSA and FCS_CKM.1/DH addresses key generation of AES/RSA keys. FCS_CKM.2/DH addresses distribution of session keys for AES keys. FCS_CKM.4 addresses key destruction of RSA keys. Note that keys of AES algorithms as a result of the DH key agreement are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination according to FDP_RIP.1. The allocated memory is freed as well. Random numbers needed for secure communication are addressed by FCS_RNG.1. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.
O.Authentication	User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1. User authentication via RMTs requires the use of a trusted path according to FTP_TRP.1.
O.Authorization	User identification is addressed in FIA_UID.2. The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. 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 as defined in FMT_SMR.1 and FMT_MOF.1. Requirements on the management functionality for the definition of access control policies are provided in FMT_MSA.1/ACFATD and FMT_MSA.3/ACFATD.

O.Security Management	The management functionality for the security functions of the TOE is defined in FMT_SMF.1.

Table 9: SFR sufficiency analysis

6.4.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

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

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

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	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_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH, Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA FCS_CKM.4/RSA
FCS_COP.1/HMAC-SHA1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH , Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_CKM.1/DH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1 Unsupported: FCS_CKM.4,

		substituted by FDP_RIP.1
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA , FCS_CKM.4/RSA
FCS_CKM.2/DH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_CKM.4/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA
FCS_RNG.1	None	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/ACFATD
FDP_DAU.1	None	N/A
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 FMT_MSA.3/IFF
FDP_RIP.1	None	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/ACFATD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1

FMT_MSA.1/IFF	[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/ACFATD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ACFATD FMT_SMR.1
FMT_MSA.3IFF	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/IFF FMT_SMR.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	N/A
FTA_TSE.1	None	N/A
FTP_TRP.1	None	N/A
FPT_STM.1	None	N/A

Table 10: Dependencies between TOE Security Functional Requirements

6.4.4 Justification for unsupported dependencies

The following dependencies are unsupported for the reasons given below.

FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1, FCS_CKM.1/DH, FCS_CKM.2/DH: The dependency on FCS_CKM.4 (Key destruction) is unsupported, because the mechanism for destruction of symmetric keys is part of the session establishment but not a dedicated key destruction mechanism. Keys of AES/HMAC-SHA1 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 according to FDP_RIP.1. So FDP_RIP.1 acts as a substitute to the mechanism according to FCS_CKM.4 for these temporary session keys. Therefore the mechanism is not modeled as dedicated key destruction mechanism by FCS_CKM.4 although the objective of the SFR – the destruction of the key when no longer in use – is fulfilled.
FCS_COP.1/SHA256: Hash functions do not require keys, so FCS_CKM.1 and FCS_CKM.4 are not applicable.

6.5 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components. No operations are applied to the assurance components.

6.6 Security Assurance Requirements Rationale

The Evaluation Assurance Level 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

For every security function a short identifier is specified in brackets to allow direct referencing to single items in other documents. For example, AUTH1 refers to the first item of the Authentication security function.

7.1.1 Authentication (AUTH)

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) The TOE supports authentication via username and password. This function is achieved by comparing user information input with pre-defined reference values stored in memory.
2) The TOE stores the following security attributes for individual uses:
   - User ID
   - User Level
   - SHA256 Hashes of Passwords
   - Number of unsuccessful authentication attempts since last successful authentication
   - Time when users are logging in and logging off
3) The TOE mandates the use of a trusted path for user authentication according to 1) via Remote Management Terminals (RMTs).
4) The TOE supports the detection of 3 consecutive failed authentication attempts after the last successful user authentication, the termination of the secure channel required for authentication in that case and the blocking of the related user account for authentication for at least 5 minutes.
5) The TOE requires each user to be successfully authenticated before he can perform any other TSF-mediated actions except authentication according to 1) when connecting to the TOE.
6) The TOE requires each user to be successfully identified before he can perform any other TSF-mediated actions except authentication according to 1) when connecting to the TOE. The username is used for identification of the user.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTP_TRP.1)

7.1.2 Access Control (AC)

The TOE enforces an access control by supporting following functionalities:

1) The TOE supports the association of user levels with user IDs and the association of command access levels with commands. Only one access level number can be associated with a command at a time and only one user level can be associated with a user, so the assignment is unambiguous.
2) The TOE supports up to 16 hierarchical access levels for users and commands. This function is achieved by storing numbers 0-15 as level in memory. It is not necessary to assign all possible access levels to commands or users/terminals. User level '0' is the lowest level and '15' is the highest level. The user level 'n+1' comprises all the access rights for user level 'n' plus the additional access rights for 'n+1' (if any) ('n' represents an integer value between 0 and 14).
3) The VRP policy mandates that a user can only execute a specific command if his user level is equal or higher to the command access level of the specific command.
4) The VRP policy mandates that a user cannot execute operations that would exceed his user level. This includes that – even if he would have sufficient user level to execute the corresponding command in general – he cannot modify user accounts of users with higher access level than his own user level. This also includes that – even if he would have sufficient user level to execute the corresponding command in general – he cannot modify the command access level of a command to a value above his own user level. As a consequence, a user could lower his own user level but not raise his own user level (under the assumption that he would have sufficient user level to perform changes to user accounts in general).
5) The TOE requires each user to be successfully identified before he can perform any other TSF-mediated actions except authentication according to Authentication 1) when connecting to the TOE. The username is used for identification and the user level of the user is used for access control.
6) The default value for the user level of a new user is '0'. Upon delivery of the TOE to the customer, there is a standard user account defined which is expected to be 'the administrator' of the device. So the user level for this account is '15' upon delivery. The TOE allows only users with sufficient user level to specify alternative default values or initial values for command access levels and user levels. The restrictions defined in 3) and 4) apply.

(FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.3/ACFATD, FMT_SMR.1)

7.1.3 L3 Traffic Forwarding (L3TF)

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

1) The TOE supports Layer 3 IPv4/v6 network traffic forwarding.
2) The TOE accepts network packets only when using a permitted transport protocol, when they originate from permitted source IP addresses and permitted source tcp or udp port numbers according to the ACL. The TOE forwards network packets only to permitted destination IP addresses and permited destination tcp or udp port numbers according to the ACL. Network packets not meeting these requirements will be discarded.
3) The TOE rejects network packets when either using a forbidden transport protocol, when they originate from forbidden source IP addresses or forbidden source tcp or udp port numbers according to the ACL. The TOE does not forward network packets to forbidden destination IP addresses or forbidden destination tcp or udp port numbers according to the ACL. Rejected network packets are discarded by the TOE.
4) The TOE restricts the ability to read, modify and delete entries in the ACL to users with sufficient access rights.

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

7.1.4 ACL (ACL)

The TOE supports Access Control Lists (ACLs) to filter traffic destined to the TOE to prevent internal traffic overload and service interruption. And the TOE also uses ACLs 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.

The content of ACLs is defined in VRP and then uploaded to CAP for execution.

1) The TOE supports ACLs by associating ACLs to whitelists and blacklists. This function is achieved by interpreting ACL configurations then storing interpreted values in memory.
2) The TOE supports screening and filtering traffic destined to the CPU. The CAP running on one CPU core is screening and filtering the traffic before it is sent to the VRP running on the other CPU core. By this the workload of the VRP can be reduced and availability can be enhanced. This function is

achieved by downloading blacklist ACL configurations to the CAP.

3) The TOE supports ACLs, which are based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.
4) The TOE permits 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.
5) The TOE restricts the ability to read, modify and delete entries in ACLs to users with sufficient access rights.

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

7.1.5 Cryptographic functions (CRYPTO)

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

1) The TOE supports symmetric encryption and decryption using the AES algorithm in CTR mode according to [FIPS 197] and [FIPS SP 800-38A] using key lengths of 128bits. AES-128 CTR is used for encryption and decryption within SSH communication.
2) (removed, enumeration has been kept to avoid conflicts with mappings to other documents).
3) The TOE supports asymmetric authentication of the TOE (server) to the client using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 using a key length of 2048bits. RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication for SSH according to chap. 6.6 [RFC 4253], ssh-rsa. The TOE supports asymmetric authentication of the client to the TOE (server) using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 using a key length of 2048bits. RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication for SSH according to chap. 7 [RFC 4252], 'publickey'.
4) The TOE supports data integrity generation and verification using the HMAC-SHA1 algorithm according to [RFC 2104], [FIPS 198-1] using key lengths of 160 bits. The data integrity protection mechanism is used for integrity protection for SSH communication.
5) The TOE supports hashing of data using SHA256 algorithm according to [FIPS 180-4].

6) The TOE supports generation and distribution of cryptographic keys according to diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048bits according to [RFC 4253], [RFC 3526], [PKCS#3] for SSH. The TOE generates a shared secret value with the client during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption (AES-128-CTR) and generation and verification of integrity protection information (HMAC-SHA1) for SSH communication. The key generation is performed according to [RFC 4253], chap. 7.2.
7) The TOE supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT. RSA keys generated have a key length of 2048bits and are intended for usage with RSASSA-PKCS1-V1_5.
8) The TOE supports the destruction of RSA keys by overwriting them with 0.
9) The TOE support the generation of random numbers according to ANSI X9.31, Appendix A.2.4 based on AES 128bit. The deterministic random number generator provided by the TOE corresponds to the requirements of class DRG.2 according to [AIS20]. The random numbers are used for generation of 128bit AES keys, RSA keys of 2048bit and 160bit HMAC keys.
10) The TOE supports the SSH protocol according to [RFC 4344], [RFC 4251], [RFC 4252], [RFC 4253], [RFC 4254] and the following cipher suites according to [RFC 4253]:
    - Diffie-hellman-group14-sha1 as key exchange algorithm of SSH.
    - AES-128-CTR encryption and decryption algorithm.
    - RSA (2048 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (server) to the client.
    - HMAC-SHA1 data integrity generation and verification algorithm.

(FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_CKM.1/DH, FCS_CKM.1/HMAC-SHA1, FCS_CKM.1/RSA, FCS_CKM.2/DH, FCS_CKM.4/RSA, FCS_RNG.1)

7.1.6 Communication Security (COMM)

The TOE provides communication security by the following mechanisms:

1) The TOE provides mechanisms to establish a trusted path between itself and a RMT based on the SSH2.0 protocol (SSH is sometimes also referred to STelnet). In addition, SFTP (i.e. FTP based on SSH protocol) is supported for file transfer. The SSH protocol uses the cryptographic algorithms as specified in chap. 7.1.5, item 10).
2) The TOE permits remote users to initiate communication with the TOE to

establish the trusted path.

3) The TOE supports mechanisms to verify the validity of the authentication information of SSH and can generate evidence about that which can be verified by SSH. For client authentication the TOE supports publickey authentication according to chap. chap. 7 [RFC 4252]. Server authentication is performed using RSA according to chap. 6.6 [RFC 4253], ssh-rsa.
4) The TOE denies the establishment of a trusted path in case of authentication failures or if the source IP address is prohibited to establish a trusted path according to ACL definitions.
5) The TOE supports termination of an interactive session after a given interval of user inactivity. This results in a loss of user authentication (for both, connections via console as well as via RMT).
6) The TOE makes temporary session keys stored in volatile memory inaccessible upon termination of SSH sessions.

(FDP_DAU.1, FDP_RIP.1, FTA_SSL.3, FTA_TSE.1, FTP_TRP.1)

7.1.7 Auditing (AUDIT)

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

1) The TOE supports generation of audit records for the following events:
   - Start-up and shutdown of the audit functions (The audit functionality cannot be disabled manually during operation but is only shutdown during shutdown for the device. In that case the TOE generates an audit record for shutdown of the device but not explicitly for the shutdown of the audit functionality.)
   - User login and logout
   - Adding, deleting or modifying a user account (including password reset and change of user level)
   - Password change by the user
   - Operation Authority Change
   - Session Termination
   - Adding, deleting or modifying a command group (including changes to command levels)
   - Modification of Authentication Policy
   - Resetting the device to factory settings
   - Configuration of the device (i.e. operation requests)
   - Modification of logging policy
2) The TOE records within each audit record the date and time of the event,

type of event, subject identity (of applicable) and the outcome (success or failure) of the event. The TOE provides reliable time stamps for that purpose. Depending on the definition of the event records might include the interface, workstation IP, User ID or CLI command name.

3) The TOE supports association of audit events resulting from actions of identified users with the identity of the user that caused the event.
4) The TOE allows all authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for reading audit records) to read the audit records.
5) The TOE supports log file formats binary and readable text. This function is achieved by providing output format transformation. By this the TOE provides the user with audit information suitable for interpretation.
6) The TOE writes audit event information to the NVRAM first (buffer). The TOE supports local storage of audit event information in the internal NOR flash memory, storage on USB Mass Storage media and output of audit event information to external audit servers.
7) The TOE does not support unauthorized modification of audit information.
8) The TOE restricts the ability to delete audit event information to authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for deleting audit records).
9) If the audit trail in the NVRAM buffer exceeds 100kB, the TOE automatically forwards the audit data to the permanent storage location (either NOR flash or USB mass storage devices) and clears the NVRAM buffer afterwards.
10) Audit functionality is activated by default.

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

7.1.8 Security Management (SM)

The TOE offers management functionality for its security functions. Security management functionality can either be used through LMT or RMT. For RMT the use of SSH is mandatory.

The access control mechanisms of the TOE are based on hierarchical access levels where a user level is associated with every user and terminal on the one hand and a command level is associated with every command. Only if the user level is equal or higher to a specific command, the user is authorized to execute this command. Management of security function is realized through commands. So for every management function sufficient user level is required for the user to be able to execute the corresponding command.

Modifications have to be saved; otherwise they will be lost after reboot of the TOE. The TOE loads the saved device configuration during start-up, so saved modifications are not lost by rebooting the device. After reset to factory defaults, the TOE is in the factory configuration.

The security management functionality comprises:

1) The TOE support configuration of ACLs based on IP protocol number, source and/or destination IP address, source and/or destination port number if TCP/UDP;
2) Support configuration on limiting access for remote administration by IP address;
3) The TOE supports the configuration of accepted cipher suites for SSH;
4) The TOE supports the configuration of the interval for user inactivity after that an established session is terminated;
5) The TOE supports the configuration of the minimum time a user account is blocked after failed attempts for user authentication;
6) The TOE supports the management of user accounts (creating, maintaining, deleting user accounts) and user data (username, password including password reset). The TOE supports the assignment of user levels to users and the maintenance of these user levels;
7) The TOE supports the assignment and maintenance of command access levels to commands and by this defining and maintaining command groups;
8) The TOE supports the configuration of the output host and output channel for audit data (e.g. output to external audit servers or USB mass storage devices);
9) The TOE supports activation of SSH functionality after seed has been provided to the deterministic random number generator;
10) The TOE supports definition of a hardware interface for remote administration.

(FMT_SMF.1)

8 Crypto Disclaimer

The following cryptographic algorithms are used by AR1220 to enforce its security policy:

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authentication	RSA signature	RSA: PKCS#1_V2.1, RSASSA-PKCS1-v1_5	|k|=2048		Signing (FCS_COP.1/RSA), using SHA256, applied during server authentication for SSH Verifying (FCS_COP.1/RSA), using SHA256, applied during client authentication for SSH
2	Key Generation	diffie-hellman-group14-sha1	PKCS#3 RFC3526 (2048-bit MODP Group)	|k|=2048		(FCS_CKM.1/DH), used in SSH V2.0. Generation of session keys for AES-128-CTR encryption and decryption as well as HMAC-SHA1 keys for generation and verification of integrity protection information are derived during DH key agreement according to [RFC 4253], chap. 7.
3	Key Exchange	diffie-hellman-group14-sha1	PKCS#3 RFC3526 (2048-bit MODP Group)	|k|=2048		(FCS_CKM.2/DH), used in SSH V2.0. Exchange of session keys for AES-128-CTR encryption and decryption as well as

						HMAC-SHA1 keys for generation and verification of integrity protection information are derived during DH key agreement according to [RFC 4253], chap. 7.
4	Confidentiality	AES-128 in CTR mode	AES: FIPS 197 FIPS SP 800-38A	|k|=128		Secure messaging for SSH V2.0 (FCS_COP.1/AES)
5	Integrity	HMAC-SHA1	FIPS 198-1	|k|=160		Secure messaging for SSH V2.0 (FCS_COP.1.1/ HMAC-SHA1)
6	Trusted Channel	SSH V2.0	RFC4344 RFC 4251 RFC 4252 RFC 4253 RFC 4254	-		Trusted channel using SSH V2.0 using the cryptographic algorithms specified in lines 1,2,3,4,7,8, (FTP_TRP.1) Client authentication mode is restricted to publickey. Server authentication is supported according to chap. 6.6 [RFC 4253], ssh-rsa.
7	Cryptographic Primitive	Determ. RNG DRG.2	ANSI X.9.31(aes-128)	128	[AIS20]	Generation of the random number (FCS_RNG.1)
8	Cryptographic Primitive	Generation of prime numbers for RSA	None			Miller-Rabin-Test is used as primality test.
9	Cryptographic Primitive	SHA256	SHA256: FIPS 180-4	256		FCS_COP.1/SHA256 Hashing for RSA signature for SSH Server

						authentication Hashing for password storage

Table 11: Dependencies between TOE Security Functional Requirements

9 Abbreviations, Terminology and References

9.1 Abbreviations

AAA	Authentication Authorization Accounting
ACL	Access Control List
AM	Access Management
ARP	Address Resolution Protocol
CAP	Concurrence Accelerate Platform
CC	Common Criteria
CFM	Configuration Management
CLI	Command Line Interface
CM	Command Management
EXEC	Execute Command
IC	Information Center
IM	Information Management
IPC	Inter-Process Communication
LMT	Local Maintenance Terminal
GUI	Graphical User Interface
MCU	Main Control Unit
MPU	Main Processing Unit
LPU	Line Process Unit
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SNMP	Simple Network Management Protocol

SPU	Service Process Unit
SRU	Switch Router Unit
SSH	Secure Shell
ST	Security Target
STP	Spanning-Tree Protocol
TF	Traffic Forwarding
TOE	Target of Evaluation
TSF	TOE Security Functions
VP	Virtual Path
VRP	Versatile Routing Platform
VTY	Virtual Teletype Terminal

9.2 Terminology

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

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE’s point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE. Since all user levels are assigned to commands and users and users can only execute a command if their associated level is equal or higher compared to the level assigned to a command, a user might have certain administrative privileges but lacking some other administrative privileges. So the decision whether a user is also an administrator or not might change with the context (e.g. might be able to change audit settings but cannot perform user management).

Operator: See User.

User: A user is a human or a product/application using the TOE which is able to authenticate successfully to the TOE. A user is therefore different to a subject which is just sending traffic through the device without any authentication.

9.3 References

[AIS20] W. Killmann, W. Schindler; A proposal for: Functionality classes for random number generators, Version 2.0, September 18th 2011.

[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

[AR Hardware Manual] Huawei AR120&AR150&AR160&AR200&AR500&AR510&AR1200&AR2200&AR3200&AR3600 series Enterprise Routers Hardware Description, Issue 05, Date 2016-06-15, AR120&AR150&AR160&AR200&AR500&AR510&AR1200&AR2200&AR3200&AR3600 Hardware Description.pdf (Document is not publicly available but can be obtained from Huawei Technologies Ltd. upon request)

[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 180-4] FIPS Publication 180-4: Secure Hash Standard (SHS), March 2012

[FIPS 186-4] Federal Information Processing Standards Publication, Digital Signature Standard (DSS), July 2013

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

[FIPS 198-1] Federal Information Processing Standards Publication 198-1, July, 2008

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

[FIPS SP 800-38A] NIST Special Publication 800-38A 2001 Edition

[FIPS SP 800-67] NIST Special Publication 800-67, Revision 1, Revised January 2012

[PKCS#1 PKCS#1 V2.1: RSA Cryptography Standard, RSA Laboratories, V2.1] Version 2.1, June, 2002

[PKCS#3] PKCS#3: Diffie-Hellman Key-Agreement Standard, Version 1.4, November 1, 1993

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

[RFC 3526] Request for Comments 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003

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

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

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

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

RFC 4344] Request for Comments 4344, The Secure Shell (SSH) Transport Layer Encryption Modes, January 2006

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