SECURITY TARGET FOR MTS SERIAL SWITCH V2.4

TOE Version: v9.7.202.3 (for box switch)

v9.7.202.3 (for chassis switch)

1 Introduction

This Security Target is for the evaluation of Belden Hirschmann IT MTS Series Ethernet Switches.

1.1 Security Target Identification

ST title	Belden Hirschmann IT MTS Series Ethernet Switches Security Target
Version	v 2.4
Author	Belden Hirschmann Industries (Suzhou) Co., Ltd
Date	2023-04-11

1.2 TOE Identification

TOE identification	Belden Hirschmann IT MTS Series Ethernet Switches
Firmware Version	v9.7.202.3 (for box switch) v9.7.202.3 (for chassis switch)

1.3 TOE Overview

Belden Hirschmann IT MTS Series Ethernet Switches is a network switch which provides networking capabilities/communications for enterprise and ITOT convergence networks. It consists of both hardware and software.

The core of Belden Hirschmann IT MTS Series Ethernet Switches has 2 different platforms.

1. Box switch product number includes MTS2700, MTS2800 and MTS2900 series,
2. chassis switch product number includes MTS8000 series.

All switches are based on the same software implementation, share the same CLI and use the same version control of software repository.

Belden Hirschmann IT MTS Series Ethernet Switches are classified into Box Switches and Chassis Switches based on their physical forms. The forwarding capacity of Chassis Switches is larger than Box Switches and Chassis Switches can use different LPU (Line Processing Unit) to provide different ports with several types, but there is no difference in security functionality.

All MTS series Ethernet Switches are Layer 3 switches. As such they provide support for the following routing protocols with different layer 3 switches shown below. Based on the supporting routing protocols, only **Open Shortest path first (OSPF) routing protocol is part of the evaluation**.

Model	Routing Protocols
MTS2724-4X-FP-S	Evaluated protocol: • Open Shortest path first (OSPFv2)
MTS2848-6X-E	
MTS2824-6X-E	
MTS2848-6X-S	
MTS2824-4X-S	
MTS2824F-4X-S	
MTS2832TF-4X-E	
MTS2748-6X-MP-E	
MTS2724-6X-MP-E	
MTS2948X-6Q-A	
MTS8003	
MTS8006	
MTS8010	

Table 1: Hardware models with evaluated routing protocol

1.3.1 TOE usage and major security features

Belden Hirschmann IT MTS Series Ethernet Switches are to be deployed within a physically secure environment to provide network communications.

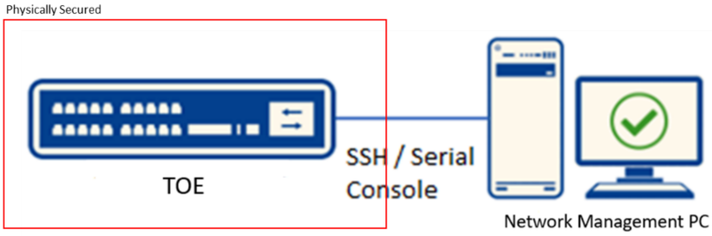

Figure 1: Network management of the TOE

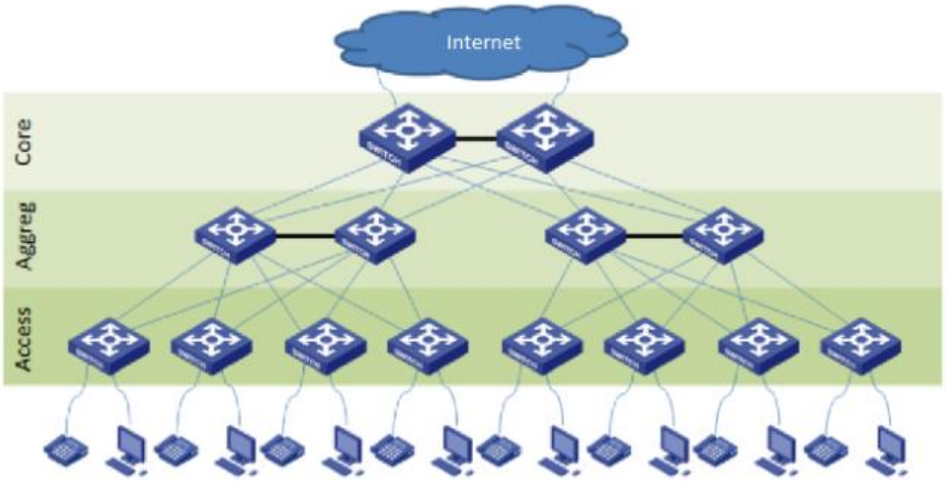

Figure 2: Network Forwarding

The evaluated Belden Hirschmann IT MTS Series Ethernet Switch shown in Figure 1 uses a PC for the TOE network communications configurations.

The switch supports both L2 and L3 forwarding shown in Figure 2.

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Authentication
- Access Control
- Information Flow Control
- Auditing
- Communication Security
- Cryptography
- Security functionality management

1.3.2TOE Type

Belden Hirschmann IT MTS Series Ethernet Switches is a network switch.

The table below states the 2 different platforms which use Box switch or Chassis switch for the TOE.

Model	Description	Interfaces
MTS2724-4X-FP-S	24*GE POE/POE+, 4*10G SFP+ slots, fixed redundancy power supply, POE output 380W	Box switch
MTS2848-6X-E	48*GE TX, 6*10G SFP+ slots, fixed redundancy power supply	Box switch
MTS2824-6X-E	24*GE TX, 6*10G SFP+ slots, fixed redundancy power supply	Box switch

MTS2848-6X-S	48*GE TX, 6*10G SFP+ slots, fixed redundancy power supply	Box switch
MTS2824-4X-S	24*GE TX, 4*10G SFP+ slots, fixed redundancy power supply	Box switch
MTS2824F-4X-S	24*1G SFP slots, 4*10G SFP+ slots, fixed redundancy power supply	Box switch
MTS2832TF-4X-E	24*1G SFP slots, 8*GE TX, 4*10G SFP+ slots, fixed redundancy power supply	Box switch
MTS2748-6X-MP-E	48*GE POE/POE+, 4*10G SFP+ slots, 1*extended line card slot, 2*Modular PSU slots	Box switch
MTS2724-6X-MP-E	24*GE POE/POE+, 4*10G SFP+ slots, 1*extended line card slot, 2*Modular PSU slots	Box switch
MTS2948X-6Q-A	1U rack mount 40G Core Switch, 48*10G SFP+ slots, 6*40G QSFP+ slots, 2*modular PSU slots, 4*FAN slots	Box switch
MTS8003	Chassis: up to 2 MPU modules of the same type, 3 LPU modules	Chassis switch
MTS8006	Chassis: up to 2 MPU modules of the same type, 6 LPU modules	Chassis switch
MTS8010	Chassis: up to 2 MPU modules of the same type, 10 LPU modules	Chassis switch

Table 2 Hardware models

1.3.3Required non-TOE hardware/software/firmware

The table below states the hardware and software requirements to support Belden Hirschmann IT MTS Series Ethernet Switches.

Hardware	
Switch	Another instance of the TOE or other switches and/or routers used to connect the TOE for L2/L3 network forward, L3 switch providing routing information to the TOE via OSPF.
Local PC	A PC for local administration via a secure channel (SSH).
Remote PC	A PC for remote administration via a secure channel (SSH).

NTP Server	A NTP to supply reliable time stamp

Table 3: non-TOE Hardware requirements

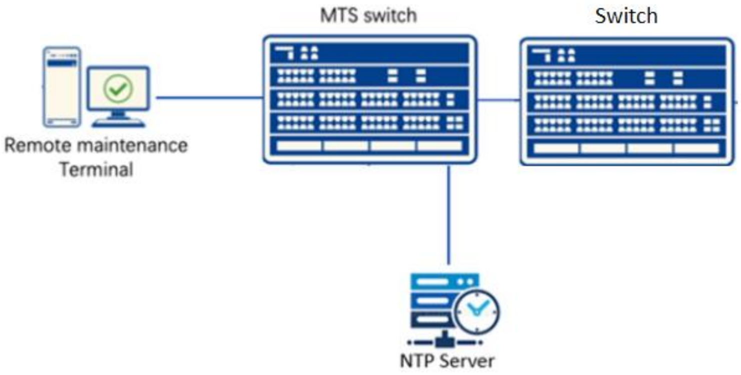

Figure 3: Non-TOE components

1.4 TOE Description

The TOE provides several models (see Table 2). These models differ in their modularity and throughput by supplying more slots in hosting chassis, but they offer exchangeable forwarding unit modules, switch fabrics, and use the same version of software. All MTS switches have the same security features and their usage to provide network communications.

1.4.1Physical Scope

The physical boundary of the TOE is the actual switch system itself.

The table below lists the TOE deliverables and their corresponding delivery methods.

Items	Description	Format	Delivery method
Safety and general information guide v1.0	Safety information regarding the setting up of the switch.	Hardcopy print	Packaged with the switch and delivered by courier service
Operational installation user guidance v1.0	Quick start user manual installation	PDF	By Belden Trusted website
User Manual 1.3	Configuration MTS serial Switch	PDF	By Belden Trusted website
Belden Hirschmann IT MTS Series Ethernet Switches	Box switch/Chassis switch	Hardware	By courier service

Table 4: TOE deliverables and delivery methods

1.4.2 Logical Scope

This section describes the logical security features of TOE.

Security Features	Description
Authentication	The TOE can authenticate administrative users by username and password. It provides a local authentication scheme for this. Authentication is always enforced for virtual terminal sessions via SSH.
Information Flow Control	The forwarding engine of the TOE controls the flow of network packets by making (and enforcing) a decision regarding the network interface that a packet gets forwarded to. These decisions are made based on a routing table that is either maintained by administrators (OSPF static routing) or gets updated dynamically by the TOE when exchanging routing information with peer routers.
Auditing	TOE generates audit records for security-relevant management actions and stores the audit records in TOE. For security management purposes, the administrators can select which events are being audited by enabling auditing for individual modules (enabling audit record generation for related to functional areas), and by selecting a severity level. Based on the hard-coded association of audit records with modules and severity levels, this allows control over the types of audit events being recorded. Review functionality is provided via the command line interface, which allows administrators to inspect the audit log.
Communication Security	The TOE provides communication security by implementing SSH protocol. SSH2 (SSH2.0) is implemented. To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH provides: • Authentication by password • AES encryption algorithms • Secure cryptographic key exchange by DH-group-exchange-sha256 • HMAC-SHA256 is used as verification algorithm for SSH
Access Control	Access Control for authenticated users by supporting the following functionalities

	• Support role-based user management • Support assigning access level to commands • Support assigning access level to user token • Support limiting executing commands
Cryptographic functions	Cryptographic functions are required by security features as dependencies, where: • Supports encryption algorithms, such as AES encryption, for SSH; • HMAC-SHA256 is used as verification algorithm for SSH; • SHA256 is used as verification algorithm for packets of OSPF; • AES Key generation
Security functionality management	Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. Other functionalities include: • Setup to enable SSH • Setup to enable authentication for OSPF • Setup to enable audit, as well as suppression of repeated log records • create, delete, and modify rules for ACL configuration

2 CC Conformance Claim

This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The CC version of [CC] is 3.1R5. The TOE claims EAL2 augmented with ALC_FLR.2. No conformance to a Protection Profile is claimed.

3 TOE Security problem definition

3.1 Threats

The information assets to be protected are the information stored, processed, or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, audit records) 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.

The threats to the TOE are identified and detailed in the following Table.

Threat Name	Threat Definition
T.UnwantedNetworkTraffic	Unwanted/malicious network traffic designated to the TOE or pass through the TOE jeopardizes the integrity of the TOE, causing the traffic flows to unauthorized destinations
T.UnauthenticatedAccess	An unauthenticated user of the TOE gains access to the TOE.
T.UnauthorizedAccess	A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. This threat also includes data leakage to non-intended person or device
T.Eavesdrop	An eavesdropper (remote attacker) can intercept, and potentially modify or re-use information assets that are exchanged between TOE and local/remote PC for management.

Table 5: Threats

3.2 Assumptions

Assumption Name	Definition
A.Time	An NTP server shall be deployed to provide reliable timestamp to the TOE.
A.PhysicalProtection	It is assumed that the TOE (including console interface used for initial configuration, access of storage device) is protected against unauthorized physical access.
A.NeworkElements	The environment is supposed to provide supporting mechanism to the TOE:

	• Peer switches or router(s) that have been configured with the TOE for the exchange of dynamic routing information through OSPF. • A remote/local entity (PCs) used by administrators of the TOE. • A NTP server for providing reliable timestamp (A.Time) These entities are considered trusted and will not attack the TOE.
A.NOEVIL	The authorized users will be competent, not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Table 6: Assumptions

3.3 Organizational Security Policy

There are no OSPs.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.UserAvail**: The TOE shall ensure only authorized users can access network resources through the TOE.
- **O.DataFilter**: The TOE shall ensure that only allowed traffic goes through the TOE.
- **O.Communication**: The TOE shall ensure secure channel for network communication between the TOE and local/remote management PC
- **O.Authorization**: The TOE shall ensure only users with the correct authorization levels access the authorized functions within the TOE.
- **O.Authentication**: The TOE shall ensure users are identified and authenticated before the users can assess the TSF functions.
- **O.Audit**: The TOE shall provide functionality to generate audit records for security-relevant administrator actions.

4.2 Objectives for the Operational Environment

- OE.NetworkElements: The operational environment shall provide secure and correctly working network devices as resources that the TOE needs to cooperate with. The behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other configured routers/switches for the exchange of routing information, NTP server for reliable timestamp, and PCs (local or remote) used by TOE administrators.
- OE.Physical: The TOE shall be protected against unauthorized physical access.
- OE.Person: Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE.
- OE.Time: A NTP server shall be deployed to provide reliable timestamp to the TOE.

4.3 Security Objectives Rationale

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.

Threat	Rationale for security objectives to remove threats
T.UnwantedTraffic	The threat is countered by O.UserAvail which ensures only authorized user can access the network and O.DataFilter ensuring that unwanted data is filtered and cannot access/jeopardize the network resources.
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). In addition, login attempts are

	logged allowing detection of attempts illegal access. (O.Audit)
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts illegal access (O.Audit)
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSHv2 for communication between the TOE and local/remote management PC (O.Communication)

Table 7: Threats to objective rationale

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

Environmental Objective	Assumption
OE.NetworkElements	A.NetworkElements
OE.Physical	A.PhysicalProtection
OE. Person	A.NOEVIL
OE.Time	A.Time

Table 8: Operational environment to Assumption

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 Conventions

The following conventions are used for the completion of operations:

- Strikethrough indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- Bold text indicates the completion of an assignment.
- Italicized and bold text indicates the completion of a selection.
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/AES"), or by appending the iteration number in parenthesis, e.g. (1), (2), (3).

6.2 TOE Security Functional Requirements

6.2.1Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1 **Audit data generation**

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamp

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) Specifically defined auditable events listed in Table 1: Auditable events

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)**

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions.	No additional information.

	Add user, change user level, or add service	
FAU_GEN.2	None	No additional information.
FAU_SAR.1	None	No additional information.
FAU_SAR.3	None	No additional information.
FAU_STG.1	None	No additional information.
FAU_STG.3	None	No additional information.
FCS_COP.1/RSA	None	No additional information.
FCS_COP.1/AES	None	No additional information.
FCS_COP.1/HMAC-SHA256	None	No additional information.
FCS_CKM.1/PKF	None	No additional information.
FCS_CKM.1/AES	None	No additional information.
FCS_CKM.1/HMAC_SHA256	None	No additional information.
FCS_CKM.4 Cryptographic key destruction	None	No additional information.
FDP_IFC.1 **Subset information flow control - Data plane traffic**	None	No additional information.
FDP_IFF.1 **Simple security attributes - Data plane traffic control**	The events of packets dropped will be recorded.	No additional information.
FDP_ITC.1	None	No additional information.
FDP_ACC.1	None	No additional information.
FDP_ACF.1	None	No additional information.
FIA_AFL.1	Failed attempts will be recorded.	The recorded message includes source IP address, username, and time stamp.

FIA_ATD.1	None	No additional information.
FIA_UAU.1	None	No additional information.
FIA_UID.1	None	No additional information.
FMT_MOF.1	None	No additional information.
FMT_MSA.1	None	No additional information.
FMT_MSA.3	None	No additional information.
FMT_SMF.1	All violations will be recorded.	The contents depend on the detailed configuration of each security function.
FMT_SMR.1	None	No additional information.
FTA_SSL.3	Terminated session will be recorded.	No additional information.
FTA_TSE.1	None	No additional information.
FTP_TRP.1	None	No additional information.

Table 9: Auditable Events

6.2.1.2 FAU_GEN.2 User identity association

FAU_GEN.2 **User identify association**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1 **Audit review**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide **Administrator and Network Admin** 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.

Application note: Only Administrator can delete the audit records.

6.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3 **Selectable audit review**

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.2.1.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1 **Protected audit trail storage**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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*** unauthorized modifications to the stored audit records in the audit trail.

Application note: Only Administrator and Network Admin can delete the logs. In the event if the size of the logs exceeds the size of the log's capacity, FAU_STG.3.1 will be triggered to overwrite the oldest logs

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

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

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

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

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_COP.1/RSA

FCS_COP.1/RSA **RSA Cryptographic operation**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA The TSF shall perform **signature generation and verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 bits** that meet the following: **RFC 4716**

6.2.2.2 FCS_COP.1/AES

FCS_COP.1/AES **AES Cryptographic operation**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AES The TSF shall perform **decryption and encryption** in accordance with a specified cryptographic algorithm **AES CTR Mode** and cryptographic key sizes **128bits, 192bits, 256bits** that meet the following: **FIPS 197**

6.2.2.3 FCS_COP.1/HMAC-SHA256

FCS_COP.1/HMAC-SHA256 **HMAC-SHA256 Cryptographic operation**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HMAC-SHA256 The TSF shall perform **authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA256** and cryptographic key sizes **256 bits** that meet the following: **RFC 2104**

6.2.2.1 FCS_CKM.1/PKF

FCS_CKM.1/PKF **Public Key Fingerprints Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/PKF The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSH key derivation** and specified cryptographic key sizes 2048 **bits** that meet the following: **RFC 4716**

6.2.2.2 FCS_CKM.1/AES

FCS_CKM.1/AES **AES Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSH key derivation** and specified cryptographic key sizes **128bits, 192bits, 256bits** that meet the following: **RFC 4344**

6.2.2.3 FCS_CKM.1/HMAC_SHA256 Cryptographic key generation

FCS_CKM.1/HMAC_SHA256 **HMAC_SHA256 Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/HMAC_SHA256 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **SSH key derivation** and specified cryptographic key sizes **256 bits** that meet the following: **RFC 4253**

6.2.2.4 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 **Cryptographic key destruction**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

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

6.2.3 Data Protection (FDP)

6.2.3.1 FDP_ACC.1

FDP_ACC.1 **Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 The TSF shall enforce the **administrator SFP** on

Subject: Administrator, Security Admin

Object: Certificate

Operation: Import

6.2.3.1 FDP_ACF.1

FDP_ACF.1 **Security attribute-based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the **administrator SFP** to objects based on the following:
Subject: **Administrator, Security Admin**

Object: **certificate**

Security attributes: **roles**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only Administrator and Security Admin is allowed to import certificate.

FDP_ACF.1.3 The TSF shall explicitly authorise 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 following additional rules: **none**

6.2.3.2 FDP_ITC.1

FDP_ITC.1 **Import of user data without security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_IFC.1 Subset information flow or FDP_ACC.1 Subset access control]

FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the **administrator SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**

6.2.3.3 FDP_IFC.1

FDP_IFC.1 **Subset information flow control- Data plane traffic control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **ACL** on

Subject: Source IP address

Operation: Transmit to destination IP address

Information: Traffic

6.2.3.4 FDP_IFF.1

FDP_IFF.1 **Simple security attributes – Data plane traffic control**

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control or
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the **ACL** based on the following types of subject and information security attributes:

Subject: Source IP address

Information: Traffic

Security attributes: Source IP address, Destination IP address, protocol type, Source port, Destination port, MAC address

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

- **If security attributes of incoming traffic are equal to user-configured security attributes, the traffic is allowed to flow to the destination IP address.**

- **Otherwise, the traffic shall be denied.**

FDP_IFF.1.3 The TSF shall enforce the **none**.

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**.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1 **Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***3*** unsuccessful authentication attempts related to **user authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **lock the user account or IP address for 10 minutes**.

Application note: FIA_AFL.1.1, FIA_AFL.1.2 – A authentication login attempts failure of consecutive 3 times in a row on a single IP or by a singe user will block the IP address or user for 10 minutes. After 10 minutes, the unsuccessful authentication counter will reset.

6.2.4.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1 **Verification of secrets**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. **Minimum 8 characters with**

- **Upper case**
- **Lower case**
- **Numbers**

6.2.4.1 FIA_ATD.1 User attribute definition

FIA_ATD.1 **User attribute definition**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.4.2 FIA_UAU.1 Timing of authentication –Administrator Authentication

FIA_UAU.1 **Timing of authentication –Administrator Authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **establishment of a secure channel between the user and TOE** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.3 FIA_UID.1 Timing of identification – Administrator Identification

FIA_UID.1 Timing of identification – Administrator Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow **establishment of a secure channel between the user and TOE** on behalf of the user to be performed before the user is identified

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

Operations/Roles	Administrator	Security Admin	Network Admin	Audit Admin	Network Operator
Network Configuration	• OSPF configuration • import Cert		• OSPF configuration • import Cert	• Show current configuration	
ACL Management	• Permit/deny protocol • Access control rules • Port control • Show port security		• Permit/deny protocol • Access control rules • Port control • Show port security		• Show port security
Audit Records	• Clear logs • Show logs		• Clear logs • Show logs		
User management	• Create user • Show user • Set Role	• Create user • Show user • Set Role			

	- Set password wrong try counter - Set password complexity	- Set password wrong try counter - Set password complexity			

Application note: All administrators roles upon successful login can unblock IP or unblock user .

6.2.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 **Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) **Network Configuration**
b) **ACL Management**
c) **Audit Records**
d) **User management**

Application note: refer to section 8.4 for detailed list of commands

6.2.5.3 FMT_SMR.1 Security roles

FMT_SMR.1 **Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

Application note: the administrator-defined roles are Administrator, Security admin, Network Operator, Network admin and Audit admin.

6.2.6TOE access (FTA)

6.2.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3 **TSF-initiated termination**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after **a time interval of user inactivity which can be configured. SSH session will be terminated after a 5 mins of user inactivity.**

6.2.6.1 FTA_TSE.1 TOE session establishment

FTA_TSE.1 **TOE session establishment**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) **Signature verification failure**
b) **Source IP address doesn't match IP address configured in ACL for user management.**

6.2.7Trusted Path/Channels (FTP)

6.2.7.1 FTP_TRP.1 Trusted path

FTP_TRP.1 **Trusted path**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

Application Note: Trusted path is related to SSH.

6.3 Security Functional Requirements Rationale

6.3.1 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	Fulfilled by OE.Time
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/RSA	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/RSA FCS_CKM.4
FCS_COP.1/AES	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/AES FCS_CKM.4
FCS_COP.1/HMAC-SHA256	FCS_CKM.1	FCS_CKM.1/HMAC_SHA256

	FCS_CKM.4	FCS_CKM.4
FCS_CKM.1/AES	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/AES FCS_CKM.4
FCS_CKM.1/PKF	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/AES FCS_CKM.4
FCS_CKM.1/HMAC_SHA256	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/HMAC_SHA256 FCS_CKM.4
FCS_CKM.4	FCS_CKM.1	FCS_CKM.1/AES FCS_CKM.1/HMAC_SHA256
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3 is not required as no SSH connection will be established without importing of client cert.
FDP_ITC.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3 is not required as no SSH connection will be established without importing of client cert.
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3 is not required as by default there is no entry in ACL list. Only when ACL list is filled with the attribute data then data can flow.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No Dependencies	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No Dependencies	None
FMT_MOF.1	FMT_SMF.1	FMT_SMF.1

	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None

Sufficiency and coverage

Objective	SFRs	Rationale
O.UserAvail	FIA_UAU.1 FIA_UID.1	These SFRs provides identification and authentication which only allows authorized users to gain access through the TOE
	FDP_IFC.1 FDP_IFF.1	These SFRs also apply ACL to limit both packets going to the Control/Management Plane and through the TOE further ensuring integrity of TOE and network resources.
O.Communication	FTP_TRP.1	This SFR provides the secure communication between users and management interface of the TOE
	FCS_COP.1/* FCS_CKM.1/* FCS_CKM.4	These SFRS provide the cryptographic services for the secure communication above.
O.DataFilter	FDP_IFC.1 FDP_IFF.1	These SFRs apply ACL to limit both packets going to the Control/Management Plane and through the TOE and thereby ensure that only protected traffic goes through.
O.Authentication	FIA_UID.1 FIA_UAU.1	These SFRs ensure that a user must identify and authenticate himself by local password
	FIA_AFL.1 FTA_TSE.1 FTA_SSL.3	The SFRs support authentication by: • Refusing logins from certain IP addresses • Not allowing unlimited login attempts

		• Logging out users after an inactivity period
O.Authorization	FMT_SMR.1 FIA_ATD.1 FDP_ITC.1 FDP_ACC.1 FDP_ACF.1	These SFRs define authorization roles and ensure that upon login an administrator gets the proper authorization level.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization level.
O.Audit	FAU_GEN.1, FAU_GEN.2	These SFRs ensure that audit records can be generated of significant events and that these contain useful information, including the correct time of the events.
	FAU_SAR.1, FAU_SAR.3	These SFRs ensure that the correct users can read the correct information from the audit records.
	FAU_STG.1, FAU_STG.3	These SFRs ensure the audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.

6.4 Security Assurance Requirements

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

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 2+ augmented with ALC_FLR.2, has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functional Specification

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

7.1.1Authentication

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:

a) Support authenticates user login using SSH by password authentication. This function is achieved by performing authentication for SSH user.
b) Support logout when no operation is performed on the user session within a given interval. This function is achieved by performing count-down through timing related to clock function.
c) Support max attempts due to authentication failure within certain period of time (default 5 minutes - configurable). This function is achieved by providing counts on authentication failure.
d) Support for user individual attributes in order to achieve all the enumerated features: user ID, user level.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FTA_SSL.3, FTP_TRP.1, FTA_TSE.1)

7.1.2 Information Flow Control

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

a) Support OSPF protocol. This function is achieved by providing implementation of OSPF protocol.
b) OSPF supports cryptographic algorithm SHA256. This function is achieved by performing verification for incoming OSPF packets using SHA256 algorithm.
c) ACL to deny unwanted network traffic to pass through itself. IP-based ACL is provided for this situation to identify traffic flow by matching all or part of IP source address, IP destination address, IP protocol number, TCP/UDP source port number, TCP/UDP destination, and port number.

(FDP_IFC.1, FDP_IFF.1)

7.1.3 Auditing

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

a) Support classification based on severity level. This function is achieved where logging messages are encoded with severity level and output to log buffer.
b) Support enabling, disabling log output. This function is achieved by interpreting enable/disable commands and storing results in memory. Log output is performed based on this result.
c) Support redirecting logs to various output channels: monitor, log buffer, trap buffer, log file. This function is achieved by interpreting commands and storing results in memory or in log files in storage device. Log channel for output is selected prior to execution of redirecting.
d) Support log output screening, based on filename. This function is performed by providing filtering on output.
e) Support querying log buffer. This function is achieved by performing querying operation with conditions input.
f) Support cleaning log buffer. This function is achieved by cleaning log buffer in memory.
g) Support to automatically remove the oldest log file if the space of the storage device storing the log files is full.
h) Only the authorized administrators can monitor the logfile record, and operate the log files. The unauthorized users have no access to do those actions. And the actions of the authorized administrators will be logged.

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

7.1.4Communication Security

The TOE provides communication security by implementing SSH protocol. SSHv2 (SSH2.0) is implemented. SSH2 is used for all cases by providing more secure and effectiveness in terms of functionality and performance.

a. Devices that can function as client and server support SSHv2. enables users to remotely and securely log in to the device and provides the interactive configuration interface.
b. Support diffie-hellman-group-exchange-sha256 as key exchange algorithm of SSH. This function is achieved by providing implementation of diffie-hellman-group-exchange-sha256 algorithm.
c. Support AES encryption algorithm. This function is achieved by providing implementation of AES algorithm.
d. Support SHA256 verification algorithm. This function is achieved by providing implementation of SHA256 algorithm.
e. Support HMAC-SHA256 verification algorithm. This function is achieved by providing implementation of HMAC-SHA256 algorithm.
f. Support using different encryption algorithms for client-to-server encryption and server-to-client encryption. This function is achieved by interpreting related commands and storing the result in memory.
g. Support for Public Key Fingerprint key construction and destruction by overwriting it with 0. (FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4/*, FMT_SMF.1) 8) Support for AES/HMAC_SHA256/DHKey construction and destruction by Releasing Memory.

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

7.1.5Security Functionality Management

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

1. Network Configuration
2. ACL Management
3. Audit Records
4. User management

All of these management options are typically available via the management workstation.

(FMT_SMF.1, FMT_MOF.1, FMT_SMR.1, FDP_ITC.1, FDP_ACC.1, FDP_ACF.1)

7.1.6Cryptographic functions

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

a) Support AES /RSA algorithms. This is achieved by providing implementations of AES /RSA algorithms.
b) Support HMAC-SHA256 algorithms. This is achieved by providing implementations of HMAC-SHA256 algorithms.
c) Support for RSA key construction and destruction overwriting it with 0 (FCS_COP.1/*, FCS_CKM.1/*, FCS_CKM.4)
d) Support for AES/HMAC_SHA256/DHKey construction and destruction by Releasing Memory

e) Support diffie-hellman-group-exchange-sha256 algorithm as key exchange algorithm of SSH

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

8 Abbreviations, Terminology and References

8.1 Abbreviations

CC	Common Criteria
CLI	Command Line Interface
IS-IS	Intermediate System to Intermediate System
LMT	Local Maintenance Terminal
LPU	Line Process Unit
NE	NetEngine
NMS	Network Management System
NSP	Network Service Processor
OFC	Optical Flexible Card PIC Physical Interface Card
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFE	Switch Fabric Extend unit
SFR	Security Functional Requirement
SFU	Switch Fabric Unit
NTP	Server Network Time Protocol Server
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
AES	Advanced Encryption Standards
RSA	Rivest Sharmir Adleman
AES	Advanced Encryption Standard Rivest Shamir Adleman

VRP	Virtual Routing Platform
MPU	Main Processing Unit

8.2 Terminology

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

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

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3. Version 3.1 Revision 5, September 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, September 2017

8.4 List of Commands

8.4.1 Audit logs commands

```
# clear logging [ buffer | file ]

# clear logging syslog [ buffer | file ]

# show logging [ buffer | file ]

# show logging filter

# show logging [ syslog ] message-counter

# show logging syslog [ file ]

# show logging time / level
```

8.4.2 Import of cert commands

```
# filesystem

# copy ftp 192.168.1.1 admin private1 authorized_key file-system authorized_key

# crpyto ca identity test

# crpyto ca import certicate to test

# ip ftp secure-identity test

# show crypto ca certificates
```

8.4.3 Access control list commands

```
# ip access-list standard { access-list-number | access-list-name }

# [ sequence ] permit { any | source-addr source-wildcard | host source-addr } [ time-range time-range-name ] [ l3-action-group l3-action-group-name ] [ egr-action-group egr-action-group-name ] [ vfp-action-group vfp-action-group-name ]

# [ sequence ] deny { any | source-addr source-wildcard | host source-addr } [ time-range time-range-name ] [ l3-action-group l3-action-group-name ] [ egr-action-group egr-action-group-name ] [ vfp-action-group vfp-action-group-name ]

# [ sequence ] remark comment

# access-list access-list-number { permit | deny } { any | source-addr source-wildcard | host source-addr } [ time-range time-range-name ] [ l3-action-group l3-action-group-name ] [ egr-action-group egr-action-group-name ] [ vfp-action-group vfp-action-group-name ]

# access-list access-list-number remark comment

# ip access-list extended { access-list-number | access-list-name }

# [ sequence ] permit protocol { any | source-addr source-wildcard | host source-addr } [ operator source-port ] { any | destination-addr destination-wildcard | host destination-addr } [ operator destination-port ] [ ack | fin | psh | rst | syn | urg ] [ precedence precedence ] [ tos tos ] [ dscp dscp ] [fragments] [ time-range time-range-name ] [ l3-action-group l3-action-group-name ] [ egr-action-group egr-action-group-name ] [ vfp-action-group vfp-action-group-name ]

# [ sequence ] deny protocol { any | source-addr source-wildcard | host source-addr } [ operator source-port ] { any | destination-addr destination-wildcard | host destination-addr } [ operator destination-port ] [ ack | fin | psh | rst | syn | urg ] [ precedence precedence ] [ tos tos ] [ dscp dscp ] [fragments] [ time-range
```

time-range-name] [l3-action-group l3-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# [sequence] remark comment

# access-list access-list-number { permit | deny } protocol { any | source-addr source-wildcard | host source-addr } [operator source-port] { any | destination-addr destination-wildcard | host destination-addr } [operator destination-port] [ack | fin | psh | rst | syn | urg] [precedence precedence] [tos tos] [dscp dscp] [fragments] [time-range time-range-name] [l3-action-group l3-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# access-list access-list-number remark comment

# mac access-list standard { access-list-number | access-list-name }

# [sequence] permit { any | source-addr source-wildcard | host source-addr } [time-range time-range-name] [l2-action-group l2-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# [sequence] deny { any | source-addr source-wildcard | host source-addr } [time-range time-range-name] [l2-action-group l2-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# [sequence] remark comment

# access-list access-list-number { permit | deny } { any | source-addr source-wildcard | host source-addr } [time-range time-range-name] [l2-action-group l2-action-name] [egr-action-group egr-action-name] [vfp-action-group vfp-range-name]

# access-list access-list-number remark comment

# mac access-list extended { access-list-number | access-list-name }

# [sequence] permit { any | source-addr source-wildcard | host source-addr } { any | destination-addr destination-wildcard | host destination-addr } [ether-type type] [cos cos] [vlan-id vlan] [time-range time-range-name] [l2-action-group l2-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# [sequence] deny { any | source-addr source-wildcard | host source-addr } { any | destination-addr destination-wildcard | host destination-addr } [ether-type type] [cos cos] [vlan-id vlan] [time-range time-range-name] [l2-action-group l2-action-group-name] [egr-action-group egr-action-group-name] [vfp-action-group vfp-action-group-name]

# [sequence] remark comment

```
# access-list access-list-number { permit | deny } { any | source-addr source-wildcard | host source-addr } { any | destination-addr destination-wildcard | host destination-addr } [ ether-type type ] [ cos cos ] [ vlan-id vlan ] [ time-range time-range-name ] [ l2-action-group l2-action-group-name ] [ egr-action-group egr-action-group-name ] [ vfp-action-group vfp-action-group-name ]

# access-list access-list-number remark comment
```

8.4.4 Create user role commands.

```
# role role-name

# rule number { deny | permit } feature {all | feature-name }

# local-user user-name class manager

# local-user user-name class network

# password 0 password

# service-type { ssh | telnet | console | ftp | web}

# user-role role-name

# group group-name

# privilege privilege-level-number

# password-control livetime

# password-control max-try-time

# max-try-time-number

# max-online-num user-number

# filesys-control{read | write | execute | none}

# work-directory directory

# service-type { xauth }

# group group-name

# stat { active / block }

# manager-group group-name

# user-group group-name

# parent group-name
```

# password-control complexity {min-length len| with user-name-check | composition type-number type-number }

# password-control firstmodify enable

8.4.5 Local User Management monitoring and maintaining command

# debug user { manager | network}

# show users class { manager | network } [username]

# show role [rolename]

8.4.6 Login Security service command

# login-secure check-record-interval check-record-interval-number

# login-secure forbid-time forbid-time-number

# login-secure max-try-time max-try-time-number

# login-secure record-aging-time record-aging-time-number

# login-secure quick-connect max-times max-times-number

# login-secure quick-connect restrict-interval restrict-interval-number

# login-secure quick-connect unrestrict-interval unrestrict-interval-number

8.4.7 Port Security rule command

# link-aggregation link-aggregation-id

# port-security enable

# port-security permit mac-address mac-address-value [desc security-rule-description | ip-address ip-address-value [desc security-rule-description] | vlan-id vlan-id [desc security-rule-description]]

# port-security deny mac-address mac-address-value [ip-address ip-address-value | vlan-id vlan-id]

# port-security permit ip-address ip-address-value [to ip-address-value]

# port-security deny ip-address ip-address-value [to ip-address-value]

# port-security maximum maximum-number

# port-security permit mac-address sticky [mac-address-value [desc security-rule-description | vlan-id vlan-id [desc security-rule-description]]]

# port-security permit mac-address sticky mode { mac | mac-ip }

# port-security aging static

# port-security aging time time-value

# port-security violation { protect | restrict | shutdown }

# port-security use-acl

Show port security command

# show port-security

# show port-security ip-address

# show port-security mac-address

# show port-security active-address

# show port-security detect-mac

# show port-security violation log-interval

# show port-security violation-mac

8.4.8 OSPF command

# router ospf process-id

# network ip-address wildcard-mask area area-id

# router-id ip-address

# router ospf process-id [vrf vrf-name]

# area area-id stub [no-summary]

# area area-id default-cost cost-value

# area transit-area-id virtual-link neighbor-id [[authentication [message-digest | null] | authentication-key key | message-digest-key key-id md5 key] / dead-interval seconds hello-interval seconds / retransmit-interval seconds / transmit-delay seconds]

# ip ospf network broadcast

# ip ospf network point-to-point

# ip ospf network non-broadcast

```
# router ospf process-id [ vrf vrf-name ]

# neighbor neighbor-ip-address [ cost cost-value / priority priority-value / poll-interval interval-value ]

# ip ospf network point-to-multipoint [ non-broadcast ]

# neighbor neighbor-ip-address [ cost cost-value / priority priority-value / poll-interval interval-value ]

# ip ospf authentication message-digest

# ip ospf message-digest-key 1 hmac-sha256 { 0 } admin

# ip ospf [ ip-address ] authentication-key { 0 | 7 } password

# ip ospf [ ip-address ] key-chain key-chain name

# ip ospf [ ip-address ] message-digest-key key-id {SHA256} { 0 | 7 } password

# redistribute protocol [ protocol-id ] [ metric metric-value / metric-type metric-type / tag tag-value / route-map route-map-name / match route-type ]

# default-information originate [ always / metric metric-value / metric-type metric-type / route-map route-map-name ]

# host ip-address area area-id [ cost cost ]

# area area-id range ip-address/mask-length [ advertise [ cost cost ] | cost cost | not-advertise ]summary-address ip-address mask [ not-advertise | tag tag-value ]

# area area-id filter-list { access { access-list-name | access-list-number } | prefix prefix-list-name } { in | out }

# distribute-list { access-list-name | access-list-number | prefix prefix-list-name } out [ routing-protocol [ process-id ] ]

# auto-cost reference-bandwidth reference-bandwidth

# distance { distance [ ip-address wildcard-mask ] [ access-list-name | access-list-number ] | ospf { external distance | inter-area distance | intra-area distance } }

# ip ospf [ ip-address ] cost cost-value

# maximum-path max-number

# ip ospf [ ip-address ] hello-interval interval-value

# ip ospf [ ip-address ] dead-interval interval-value

# passive-interface { interface-name [ ip-address ] | default }
# ip ospf priority priority-value

# ip ospf [ ip-address ] mtu-ignore

# ip ospf transmit-delay delay-value

# ip ospf retransmit-interval interval-value

# ip ospf database-filter all out
```

8.4.9 OSPF monitoring and maintaining command

```
# clear ip ospf [ process-id ] process

# clear ip ospf process-id neighbor neighbor-ip-address [ neighbor-router-id ]

# clear ip ospf statistics [ interface-name ]

# clear ip ospf [ process-id ] redistribution

# clear ip ospf [ process-id ] route

# show ip ospf [ process-id ]

# show ip ospf [ process-id ] border-routers

# show ip ospf [ process-id ] buffers

# show ip ospf [ process-id ] database [ adv-router router-id | age lsa_age | database-summary | max-age | [ asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | self-originate | summary ] [ [ link-state-id ] [ adv-router advertising-router-id ] | self-originate | summary ] ]

# show ip ospf interface [ interface-name [ detail ] ]

# show ip ospf [ process-id ] neighbor [ neighbor-id | all | detail [ all ] | interface ip-address [ detail ] | statistic ]

# show ip ospf [ process-id ] route [ ip-address mask | ip-address/mask-length | external | inter-area | intra-area | statistic ]

# show ip ospf [ process-id ] virtual-links

# show ip ospf [ process-id ] sham-links
```