# Ciena
# Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 Security Target

Version 1.7
March 12, 2014

Prepared for:

Ciena

7035 Ridge Road

Hanover, Maryland 21076

Prepared by:

Booz Allen Hamilton

Common Criteria Testing Laboratory

900 Elkridge Landing Road, Suite 100

Linthicum, MD 21090-2950

# Table of Contents

# List of Figures



# List of Tables

# 1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

## 1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level 2 (EAL2).

### 1.1.1 ST Identification

| | |
|---|---|
| ST Title: | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 |
| ST Version: | 1.7 |
| ST Publication Date: | March 13, 2014 |
| ST Author: | Booz Allen Hamilton |

### 1.1.2 Document Organization

*Chapter 1* of this ST provides identifying information for the TOE. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

*Chapter 2* describes the TOE Description, which includes the physical and logical boundaries, and describes the components and/or applications that are excluded from the evaluated configuration.

*Chapter 3* describes the conformance claims made by this ST.

*Chapter 4* describes the Security Problem Definition as it relates to threats, Operational Security Policies, and Assumptions met by the TOE.

*Chapter 5* identifies the Security Objectives of the TOE and of the Operational Environment.

*Chapter 6* describes the Extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

*Chapter 7* describes the Security Functional Requirements.

*Chapter 8* describes the Security Assurance Requirements.

*Chapter 9* is the TOE Summary Specification (TSS), a description of the functions provided by the TOE to satisfy the SFRs and SARs.

*Chapter 10* is the Security Problem Definition Rationale and provides a rationale or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims for the chosen EAL, any deviations from CC Part 2 concerning SFR dependencies, and a mapping of threats to assumptions, objectives, and SFRs. It also identifies the items used to satisfy the Security Assurance Requirements for the evaluation.

### 1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1 and 1-2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

| Terminology | Definition |
|---|---|
| Admin | Read/Write role with Limited privileges that can also perform execute commands |
| BVID | Backbone VLAN identifier; attribute in PBB-TE |
| C-tag | Customer VLAN tag; Used to create VLANs within the customer domain |
| Control Card | Hardware card within the TOE that performs the control plane functionality |
| Control Plane | Monitors the system and maintains the signal based configuration as well as the OAM control protocols |
| Data Plane | Allows for Data flow |
| Diag | Diagnostic role with no restrictions on privileges |
| ISID | Instance Service Identifier tag; used for the classification of traffic in PBB-TE |
| Forward | The TOE's ability to associate ingress traffic with egress ports and transfer traffic by using virtual switches and/or VLANs |
| Limited | Read-only role; able to execute commands that do not change the state or configuration of the TOE |
| Line Card | Hardware card within the TOE that performs the switching functionality |
| Management Control Card | Hardware card within the TOE that performs the management plane functionality |
| Management Plane | Allows for the management of the system through user configuration |
| Middleware | Provides communication between subsystems |
| Privilege Level | Vendor-specific terminology synonymous with role |
| S-tag | Service VLAN tag |
| Service | A logical association of network traffic based upon packet headers indicative of a specific type of traffic |
| Service Aggregation Switch | Provides the aggregation of data through a network via virtual switches; as a black box, the key differentiators are port density and port speeds for scalability |
| Service Delivery Switch | Provides the delivery of data through VLANs ; as a black box, the key differentiators are port density and port speeds for scalability |
| Severity | Synonymous with log-level within audit data; Determines the likelihood of an audit event to disrupt the TOE functionality or security |
| Super | Read/Write/Create role with Admin privileges; Has user management privileges in addition to general TOE management functions |

**Table 1-1: Customer Specific Terminology**

| Term | Definition |
|---|---|
| TOE Security Functions (TSF) | A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP. |
| User | Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. |

**Table 1-2: CC Specific Terminology**

### 1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

| Acronym | Definition |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| ACL | Access Control List |
| ARP | Address Resolution Protocol |
| CAM | Content Addressable Memory |
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCIMB | Common Criteria Interpretations Management Board |
| CCM | Continuity Check Messages |
| CES | Carrier Ethernet Solutions |
| CFM | Control Frame Monitor |
| CLI | Command-line Interface |
| CIR | Committed Information Rate |
| CoS | Class of Service |
| CPU | Central Processing Unit |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EAL | Evaluation Assurance Level |
| ESM | Ethernet Services Manager |
| EUV | Egress Untagged VLAN |
| FTP | File Transfer Protocol |
| HAL | Hardware Abstraction Layer |
| IP | Internet Protocol |
| IP-ACL | IP - Access Control List |
| IPC | Inter-Process Communication |
| IT | Information Technology |
| MAC | Media Access Control |
| MD5 | RSA Message Digest 5 |
| MEP | Maintenance End Point |
| MIB | Management Information Base |
| MIP | Maintenance Intermediate Point |
| NAS | Network Access Server |
| NIAP | National Information Assurance Partnership |
| NMS | Network Management System |
| NTP | Network Time Protocol |
| OAM | Operations, Administration, and Maintenance |
| OS | Operating System |
| PBB | Provider Backbone Bridging |
| PBB-TE | Provider Backbone Bridging – Traffic Engineering |
| PDU | Protocol Description Unit |

| | |
|---|---|
| PIR | Peak Information Rate |
| PP | Protection Profile |
| PVID | Port VLAN ID |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial In User Service |
| RAM | Random Access Memory |
| RLAN | Resolved Local Area Network |
| SAOS | Service Aware Operating System |
| SAP | Service Access Point |
| SAR | Security Assurance Requirement |
| SAS | Service Aggregation Switch |
| SDS | Service Delivery Switch |
| SFP | Security Function Policy |
| SFTP | Secure File Transfer Protocol |
| SFR | Security Functional Requirement |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TACACS+ | Terminal Access Controller Access-Control System Plus |
| TFTP | Trivial File Transfer Protocol |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TWAMP | Two-Way Active Measurement Protocol |
| UDP | User Datagram Protocol |
| UTC | Coordinated Universal Time |
| VLAN | Virtual Local Area Network |

**Table 1-3: Acronym Definitions**

### 1.1.5 References

[1] SAOS 6.10.2 CLI Reference Manual

[2] SAOS 7.2 CLI Reference

[3] SAOS 6.10.2 Software Configuration Guide

[4] SAOS 7.2 Software Configuration Guide

### 1.1.6 CC Concepts

The following are CC concepts as used in this document. A Subject is any user of the TOE (users and data flow sources/destinations). An Object (i.e., resource or entity) can be a service, an IT server, a command issued by a user, etc. An Operation is any action on a resource (e.g. read, write, create, forward, or block). A Security Attribute is information such as usernames, password, roles, packet headers, physical port identifiers, etc. that is kept in the defined users and flow control policies stored within the TOE. An External Entity is anything outside of the TOE that affects the TOE.

## 1.2 TOE Reference

Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2.

## 1.3 TOE Overview

Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 (hereafter referred to as CES or the TOE) receives data from an external source and forwards that data to one or many ports. CES is part of the Carrier Ethernet technology. Carrier Ethernet provides a way to deliver Ethernet services across many networks while providing bandwidth management. CES operates on QoS capabilities and virtual switching functions to deliver different amounts of data to various ports. CES also contains next-generation Ethernet features that transport different Ethernet services through fiber or copper connections.

The TOE:

- Receives network frames from physical ports
- Associates the frames with logical services
- Queues outgoing traffic to physical ports based on the logical services
- Forwards data frames based on the allocated bandwidth

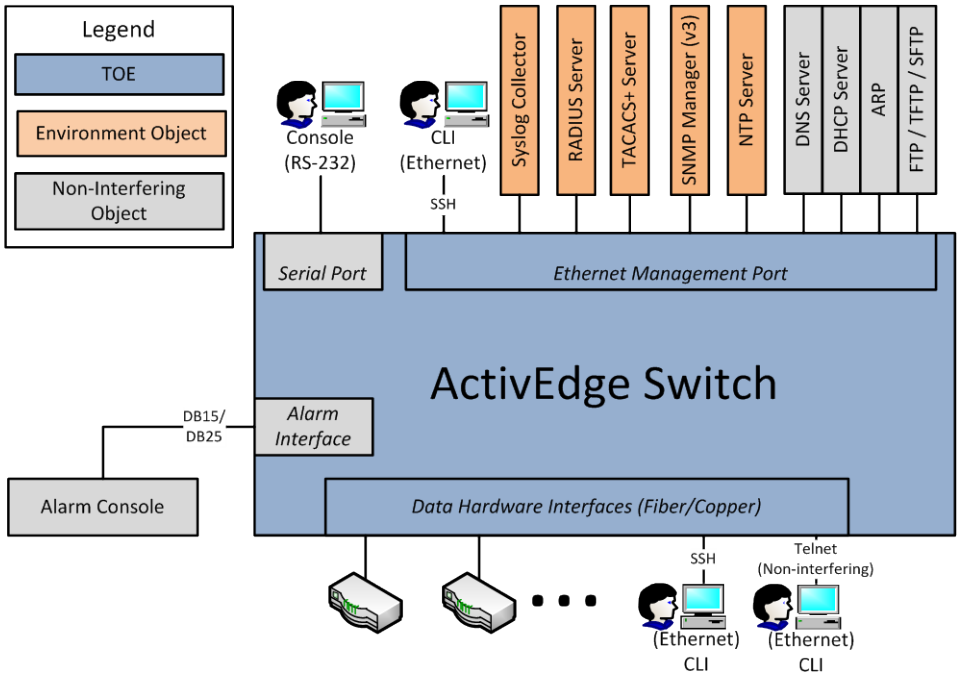


**Figure 1 – TOE Boundary**

As illustrated in Figure 1, the TOE is a single hardware device that has an Ethernet management port, a serial port, and data hardware interfaces. The data hardware interfaces provide both ingress and egress traffic. The Ethernet management port allows users to connect to the TOE via SSH through a command line interface. In addition, the management port serves as a communication channel to external entities such as RADIUS, TACACS+, and NTP servers, as well as a syslog collector and SNMP manager. It should be noted that there are several objects that are non-interfering and have been grayed-out in the diagram. These objects include the Serial Port, DNS Server, DHCP Server, ARP, FTP/TFTP/SFTP, and the Alarm Console. These objects do not offer security-relevant functionality or are used solely for initialization of the TOE. Reference the legend for Figure 1 as a reference to locate these excluded objects.

The TOE has the ability to take traffic in then transport and encapsulate it into a secure envelope which gets forwarded to various network locations and networks. Data enters the TOE on a physical port. Physical ports on the TOE are mapped to logical ports. These logical ports (also referenced as logical interfaces) are attached to virtual switches or VLANs within the TOE. The TOE will forward the data to connections that are linked to the virtual switches or VLANs. The TOE maintains queues on the egress ports as part of the Class of Service (CoS) policy. CoS allows the TOE to allocate bandwidth to certain ports and schedule the transit of data through the ports specified.

The TOE is comprised of three separate logical planes, each providing different functionality, and Middleware that allows communication between the planes. A description of each plane and Middleware is described below:

- Management plane – Manages the system through user configuration.
- Control plane – Serves as signal based configuration; provides signaling between the data plane and management plane for monitoring the TOE.
- Data plane – Handles the data flow through the TOE.
- Middleware – Allows each TOE subsystem to communicate and perform application functions within the software architecture throughout the TOE.

The TOE can connect to five components that do not offer security-relevant functionality or are used primarily during initialization. These components interact with the non-interfering Operational Environmental components on a per-service basis (i.e. DNS service communicates with the DNS server):

- DNS Client Service – Allows the TOE to forward DNS lookup requests lookup request to the appropriate DNS server for IP to Name or Name to IP resolution. In the evaluated configuration, this component does not have any effect on the TOE configuration.
- DHCP Client Service – Provides the ability to use a DHCP server to initialize the TOE. In the evaluated configuration, this component is disabled on all interfaces by default.

- ARP – Maps Ethernet MAC addresses to Destination locations such as ports, VLANs, or logical ports. In the evaluated configuration, this component does not have any effect on the TOE configuration.
- FTP/TFTP/SFTP – The FTP/TFTP/SFTP components are optional services that can be used to store various configuration, log and administration files and download them to the devices on the network. The services are not used in the evaluated configuration of the TOE.
- Alarm Console – The Alarm Console provides a method of viewing event information generated by the TOE. This feature under a process of deprecation is thus non-interfering with respect to the SFRs.

### 1.4 TOE Type

The TOE type for CES is Network Device. Network Device is defined by CCEVS as "an infrastructure device (as opposed to an end-user device) that can be connected to a network)." It is also defined as a "device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise."

# 2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

## 2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

| Component | Definition |
|---|---|
| SAOS 7.2.0.585 | The system software on CES 5410 and 5305 Service Aggregation Switches. This system software cannot be installed on Service Delivery Switches. Service Delivery Switches are intended to be deployed at the edge of a network, while Service Aggregation Switches are intended to be deployed in the network's core. This system software is based on a common Service Aware Operating System (SAOS) code base designed to deliver consistent benefits across all Ethernet delivery, aggregation, and distribution configurations.<br><br>Certain licenses may be included for additional functionality. For SAOS 7.2, the following licenses are included in the evaluated configuration:<br>• Advanced-Security<br>• PBB-TE<br>• MPLS |
| SAOS 6.10.2.140 | The system software on CES 3900 Series and 5100 Series Service Delivery Switches. Service Delivery Switches are intended to be deployed at the edge of a network, while Service Aggregation Switches are intended to be deployed in the network's core. This system software is based on a common Service Aware Operating System (SAOS) code base designed to deliver consistent benefits across all Ethernet delivery, aggregation, and distribution configurations. SAOS 6.10.2 itself is based on the Linux operating system.<br><br>Certain licenses may be included for additional functionality. For SAOS 6.10.2, the following licenses are included in the evaluated configuration:<br>• Advanced Security<br>• PBB-TE<br>• MPLS<br>• Advanced 10G<br>• Advanced Ethernet<br>• Advanced OAM |

**Table 2-1: Evaluated Components of the TOE**

## 2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

| Component | Definition |
|---|---|
| Syslog Collector | The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes. |
| RADIUS Server | This component allows for RADIUS authentication. The TOE communicates to this component to verify users and user attributes including user-groups. RADIUS authentication is appropriate for TOEs deployed within an enterprise environment. |

| | |
|---|---|
| TACACS+ Server | This component allows for TACACS+ authentication. The TOE communicates to this component to verify users, user attributes, and user-groups. TACACS+ authentication is appropriate for TOEs deployed within an enterprise environment. |
| NTP Server | This component allows communication with the TOE to provide reliable and accurate time. After configuration, the TOE will receive updated time information from the NTP Server on a regular basis. |
| SNMP Manager (v3) | This component allows the TOE to communicate with it and to send SNMP traps based on specified events. SNMP traps are sent out based upon security violations or system faults detected by the TOE. SNMP can also be used to configure the TOE when the ESM component is also utilized with the TOE. The ESM component is excluded from the evaluation, and therefore this additional functionality is not utilized. |

**Table 2-2: Evaluated Components of the Operational Environment**

## 2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

### 2.3.1 Not Installed

- Ethernet Services Manager – This is an optional module that serves as an automated service activation, creation, and management platform for the CES devices. The ESM is used as a primary viewer of appliance and endpoint status within a deployment of Carrier Ethernet devices. The Ethernet Services Manager is not part of the evaluated configuration because it provides separate enhanced functionality and is a separately purchased product.

### 2.3.2 Installed but Requires a Separate License

The licenses included in this evaluation depend on the SAOS version. The evaluated licenses for each version are as follows:

6.10.2

- Advanced Security
- PBB-TE
- MPLS
- Advanced 10G
- Advanced Ethernet
- Advanced OAM

7.2

- Advanced-Security
- PBB-TE
- MPLS

### 2.3.3 Installed But Not Part of the TSF

- Serial Port – The Serial Port is only used for initial set up and configuration of the TOE. This port is not part of the evaluated configuration because it is not intended to be used as a permanent connection. The initial configuration for this port cannot be changed and is not used in standard practice.

- Telnet – Telnet is used to remotely connect to the TOE via the Ethernet management port. Telnet is not part of the evaluated configuration as it is an insecure communication protocol. Telnet is to be disabled and SSH is to be used in its place.

- Alarm Console – The alarm console allows the TOE to trigger alarms based on the status of the TOE. An alarm console is considered to be any device connected to the TOE that stimulates an alarm from any applicable connected device. Devices can be visual or audible alarm systems. This component has been omitted from the evaluated configuration as use of the alarm console is being deprecated. Newer product lines and versions of the TOE are either not including or not supporting the alarm console.

- DNS Client Service – Allows the TOE to forward DNS lookup requests to the appropriate DNS server for IP to Name or Name to IP resolution. In the evaluated configuration, this component does not provide any changes to the TOE, the data that the TOE uses, or data that pass through the TOE. This component is not security-relevant.

- DHCP Client Service – Provides the ability to use a DHCP server to initialize the TOE. In the evaluated configuration, this component is disabled on all interfaces by default.

- ARP – Maps Ethernet MAC addresses to Destination locations such as ports, VLANs, or logical ports. In the evaluated configuration, this component does not cause any change to be made on the TOE.

- FTP/TFTP/SFTP – The FTP/TFTP/SFTP components are optional services that can be used to store various configuration, log and administration files and download them to the devices on the network. The services are not used in the evaluated configuration of the TOE.

- SNMP Management – The TOE provides the capability to send management commands through SNMP messages. This functionality is excluded from the evaluated configuration because SNMP messages are not sent in a sufficiently secure manner. The user interfaces that utilize SSH are to be used to manage the TOE.

- Diag Role – The Diag Role is the role with the most privileges. It can perform all the functions of the Super role with a few additional commands used for debugging. These additional debugging commands are not security-relevant and are not intended for use within the normal operation of the TOE. For this reason, the Diag Role is not security-relevant and is excluded from the evaluated configuration.

## 2.4 Physical Boundary

### 2.4.1 Hardware

The model specific hardware is as follows:

CES 5305

- RS-232 to Serial port (excluded)
- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- Alarm Interface
- (2) Front-Loaded Redundant Dedicated Control Modules
- (5) Front-Loaded Hot-Swappable Line Modules
- (2) Front-Loaded Hot-Swappable Power Supplies
- (1) Front-Loaded Fan Tray

CES 3900 Series

- RS-232 to Serial port (excluded)
- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- (2) Redundant Power Supplies with integrated fans

CES 5100 Series

- RS-232 to Serial port (excluded)
- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- (1) DC Input Power Supply and/or (1) AC Input Power Supply
- (1) Field Replaceable Redundant Fan Tray

CES 5410

- RS-232 to Serial port (excluded)
- (2) DCN M Redundant Ethernet Management ports
- Data Hardware Interfaces port (fiber/copper)
- Alarm Interface

### 2.4.2 Software

The TOE software is Service Aware Operating System (SAOS) 6.10.2 and 7.2.

## 2.5 Logical Boundary

The logical boundary of the TOE is described in the terms of the security functionalities that the TOE provides to the systems that utilize this product for network data aggregation, mapping and forwarding.

The logical boundary of the TOE is broken down into the following security classes: Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access, and Trusted Path/Channels. Listed below are the security functions with a listing of the capabilities associated with them:

### 2.5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record contains the user information, time stamp, message briefly describing what actions were performed, outcome of the event, and severity. All audit record information is associated with the user of the TOE (if applicable). The TOE also maintains the ability to allow an authorized user to set and configure the settings for forwarding the data to the SNMP server. The TOE allows all users to view the log files. Only users of Admin-level or above can view the commands requiring Super-level access. All audit data is displayed to users in a user-readable format. The TOE also contains mechanisms to notify the user upon detection of a potential security violation, including failed authentication, temperature threshold exceeded, fan failure, link status change, and line card failure. The TOE notifies external entities of detected faults through the usage of SNMP traps. Security violations are also recorded in the log files. Audit data generated to an external device can be configured to be sent to one or more syslog collectors. The transmission of audit data to syslog collectors is dependent on the syslog threshold configured on the TOE. The TOE does not allow any of the users to modify the audit logs. When the collector becomes full the TOE will overwrite the oldest log with the new audit information collected.

### 2.5.2 Cryptographic Support

SSHv2 is the protocol that allows connections to the TOE. SSH authentication generates a 256-bit AES key each time the user initiates with the TOE. The TOE also uses SSH to

generate the public and private key pair. Only users with the Admin role can issue commands for key generation and deletion. SSH is used by the TOE for all user sessions through the CLI and is protected using standard SSH encryption practices. The SNMP traffic, as well as password information that is either sent or stored on the TOE, is encrypted throughout transit using SNMPv3 encryption standards.

### 2.5.3 User Data Protection

The TOE's core functionality is to receive data packet frames on its physical ports, traverse the data frames through its internal flow processing functionality, and forward the traffic to an associated destination port. The TOE allocates or deallocates memory depending on the resources needed to complete the forward. The TOE also allows for authorized Admin or higher privileged users to define and map services to physical ports. In all systems where PBB-TE is used on incoming traffic, the TOE applies PBB-TE services to the ingress data frames to forward the traffic to the appropriate port. All traffic must pass through the virtual switch or VLAN in order for it to be forwarded. All VLAN traffic is forwarded based upon the tags contained within the header field. This varies between the type of VLAN traffic, of which PBB-TE is a type of traffic used. The TOE determines the order of egress traffic based on the QoS and CoS schemes.

The TOE enforces its information flow control policy based on different specifications on the system. The TOE maintains access control lists, MAC assignments, MAC learning tables, and management VLAN. These controls allow the TOE to explicitly allow and/or deny information flow throughout the TOE. Additionally, customer premise equipment can be authenticated through the use of 802.1x.

### 2.5.4 Identification and Authentication

The TOE and its configured authentication services maintain distinct user accounts which contain the following attributes: user name, password, and role. The access rights correspond with the user's role on the system within a session object. If a user becomes logged out of the TOE either through the user logging his or herself out, or because of inactivity on the TOE, the changes will be reflected immediately and the user must re-enter credentials to log in to the TOE. All users must identify and authenticate before performing any TSF-mediated actions. The TOE supports authentication through its local database, as well as through the RADIUS and/or TACACS+ services. Multiple authentication methods can be configured in a hierarchical structure to prevent access failure by enabling the next authentication method in the list when the current method fails. TACACS+ associates the privilege level with each authenticated user on the TOE. When users are entering their passwords for authentication, the TOE does not display the clear text of the password to the user, but displays an obscured character feedback such as dots. Upon failed authentication attempts, the TOE will only display a message to the user stating that the user's logon was not permitted.

### 2.5.5 Security Management

The TOE maintains distinct roles for user accounts: Limited, Admin, and Super. These roles define the management functions for each user on the TOE. The Admin role is not available in SAOS version 6.10.2. For any references to functions requiring the Admin role, it can be assumed that these functions require the Super role in SAOS version 6.10.2. The Limited user is a read-only user, so any commands the user performs on the TOE will only allow the user to view different attributes and settings. The next level role is the Admin user who can perform all system configurations with the exception of managing users. Following the Admin role is the Super role. Super users can perform all system configurations including user management, including creating and deleting users on the TOE. Users with the minimum Admin-level privilege have the ability to configure the Ciena Carrier Ethernet Flow Control SFP.

The major functional areas of the TOE include managing flow control policy, users, and general configuration. These areas are restricted to those users with necessary minimum role or higher.

### 2.5.6 Protection of the TSF

The TOE maintains a secure state upon a port-link failure by allowing a transfer of primary service links. In the event of a Control Card failure in a chassis-based TOE, the TOE has the capability to remain in a secure state. The TOE performs POSTs to ensure the system is in a fully operational mode during start-up. The TOE checks the hardware upon start-up including CPU registers and memory space. If the TOE observes any fault or error, an alert will be published to the user. The TOE's internal system clock allows the user to see an accurate time of the failure. The system clock can be kept accurate through the use of time synchronizations with external NTP servers. Fault tolerance is also applied for the failure of any Control Card. If a Control Card fails, the secondary or backup Control Card will assume the TOE functionality. The TOE maintains the ability to test its link quality and performance because the configuration file is verified on the backup Control Card. Users will not be able to verify any additional TOE information other than the status of the CPU registers and memory space information as well as the TOE configuration data.

### 2.5.7 Resource Utilization

The TOE maintains fault tolerance capabilities to maintain forwarding functionality in the occurrence of a Control Card failure in a chassis system or a service link failure in a connection with redundant physical connections. As an example, the Control Card provides a "heartbeat" to the monitoring standby card. If the "heartbeat" is lost, the standby card will then perform a switch-over to a 'mirror image' card.

The TOE uses PBB-TE or sub-ports to apply QoS schemes to the data frames sent over the system. With QoS, the TOE can provision and reserve appropriate bandwidth for each data stream to maintain a steady tunneling of traffic.

### 2.5.8 TOE Access

The TOE allows users to view a configurable banner upon establishing the user session. Only Limited users are not allowed to configure the banner for the TOE. The TOE is able to disconnect inactive users if the users' session reaches the configured inactivity time threshold. Each user can initiate the termination of the associated user session by entering the "quit" command. The TOE also has a maximum number of concurrent sessions for each user role as well as for SSH connections, and therefore can deny users access based on the number of sessions currently established.

### 2.5.9 Trusted Path/Channels

Connections to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section. Trusted paths are used to secure all CLI sessions through SSH. Users initiate the trusted path to the TOE through establishing an SSH connection. The trusted path is used for authentication and all user management functions. All connections for the TOE are protected using the SSH cryptographic mechanism.

## 2.6 Security Architecture

### 2.6.1 Security Domains

Services identified within the TOE's flow control policy can be identified on any value within any acceptable frame. With the flow control policy, service traffic can be separated into specific domains on the TOE. This is the primary goal of Carrier Ethernet. Carrier Ethernet devices assure that traffic carried by a frame does not cross into domains that would present a security risk. The TOE possesses the capability to segregate data based on the information in the data frame.

User sessions are also appropriately separated into domains, based on the username and the internal process ID for that session. The session ID linked to the username and role allow the TOE to distinguish users, such that the TOE will not allow other users to co-opt an existing session.

### 2.6.2 Secure Initialization

The TOE maintains a secure boot-up by not being operational for user management during the start-up process. The TOE user interface over SSH is not available for new connections until all other components are running. This is monitored by the TOE's equipment subsystem which notifies all modules once every module has been run. After modules receive the notification, the TOE allows them to perform normal processing functions.

### 2.6.3 Protection from Tampering

The TOE has different hardware and software mechanisms in place to protect itself from tampering depending on the model. Some devices contain hardened enclosures or doors with key locks. While the TOE's hashing and encryption techniques serve as software protection of the TOE's data.

### 2.6.4 Non-bypassability

All data processing for the TOE is done at a hardware level. During the ingress, switch, and egress processing, there is no potential for bypass. All user connections occur over encrypted SSH sessions. These connections cannot be bypassed because the SSH server is the only entity in place to accept user connections to the TOE.

# 3 Conformance Claims

## 3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2009-07-004, Version 3.1 Revision 3 July 2009.

## 3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended for EAL2 to include all applicable NIAP and International interpretations through 4 April 2011.

## 3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant for EAL2 to include all applicable NIAP and International interpretations through 4 April 2011.

## 3.4 PP Claims

This ST does not claim conformance to any Protection Profile.

## 3.5 Package Claims

This TOE has a package claim of EAL2.

## 3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are conformant to EAL2 package claims.

## 3.7 Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

# 4 Security Problem Definition

## 4.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

## 4.2 TOE Threats

| | |
|---|---|
| **T.ACCESS** | A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions. |
| **T.ADMIN_ERROR** | An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms. |
| **T.AUDIT_COMPROMISE** | A malicious user or process may view audit records, cause the records or information to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action. |
| **T.DATA_COMPROMISE** | A malicious user or process may attempt to gain unauthorized access and/or obtain resources controlled by the TOE that have been allocated during a TOE operational session. |
| **T.EAVESDROPPING** | A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. |
| **T.NETWORK_FLOW** | A malicious user may attempt to subvert the TOE or defeat the operation of its security mechanisms to cause a disruption in the flow of data on the production network. |
| **T.MASK** | Users, whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures. |
| **T.STEALTH** | A malicious user or process could perform suspicious activities against the TOE or objects in the Operational Environment monitored by the TOE without a TOE user authorized by the TOE or Operational Environment becoming aware of this. |

## 4.3 Organizational Security Policies

The TOE addresses the organizational security policy described below.

**P.ACCESS_BANNER** The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

## 4.4 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

### 4.4.1 Personnel Assumptions

**A.ADMIN** One or more users authorized by the Operational Environment will be assigned to install, configure and manage the TOE and the security of the information it contains.

**A.NOEVIL** Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.

**A.PASSWORD** Users select passwords according to the strong password policy that has been configured by an administrative user and will protect their own authentication data.

### 4.4.2 Physical Assumptions

**A.CPE** Service Delivery Switches will only be deployed to connect to Customer Premise Equipment.

**A.LOCATE** The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

**A.PROTECT** The operational environment must protect the channel to the configured syslog collectors from interruption using logical methods, such as encryption, or physical methods such as disconnecting the TOE from internet and storing it in the same secure location.

# 5 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

## 5.1 TOE Security Objectives

The following are the TOE security objectives:

**O.ACCESS** The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.

**O.ALERT** The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded.

**O.AUDIT** The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.

**O.AUTH** The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.

**O.DEALLOCATION** The TOE will provide measures to perform deallocation of memory from a TOE object when a session has been ended.

**O.DISPLAY_BANNER** The TOE will display an advisory warning regarding use of the TOE.

**O.EAVESDROPPING** The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.

**O.MANAGE** The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.

**O.MAP** The TOE will provide mechanisms to set and control the association of physical data identifiers and logical data identifiers with the TOE services.

**O.NETWORK_FLOW_PROTECTION** The TOE will preserve the information flow of the production network data through the TOE in the presence of adversarial activity when a component of the TOE fails.

| | |
|---|---|
| **O.ROBUST_TOE_ACCESS** | The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate. |
| **O.SYSTIME** | The TOE will provide reliable system time. |

### 5.2 Security Objectives for the operational environment of the TOE

The TOE's operating environment must satisfy the following objectives.

| | |
|---|---|
| **OE.ADMIN** | One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains. |
| **OE.CPE** | Service Delivery Switches must only be deployed to connect to Customer Premise Equipment. |
| **OE.LOCATE** | The TOE will be located within controlled access facilities that will prevent unauthorized physical access. |
| **OE.NOEVIL** | All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. |
| **OE.PASSWORD** | All users of the TOE will select appropriately strong passwords and will protect their own authentication data. |
| **OE.PROTECT** | All channels to the configured syslog collectors will be protected from interruption using logical (encryption) or physical (disconnecting from the internet) methods. |

# 6 Extended Security Functional and Assurance Requirements

## 6.1 Extended Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

| Security Function | Security Functional Components |
|---|---|
| Security Audit (FAU) | FAU_STG_EXT.1 External audit trail storage |

**Table 6-1: Extended Security Functional Requirements for the TOE**

### 6.1.1 Class FAU_EXT.1 External audit trail storage

#### 6.1.1.1 FAU_STG_EXT.1 Component Definition

The purpose of creating the additional requirement for data collection is to highlight the TOE's ability to send audit data to an external source. There are no current SFRs that refer to transferring audit data to an external entity. The closest requirement available is the Security Audit class requirement for audit storage. This is slightly altered to pertain to using an external source to receive the audit records.

| | |
|---|---|
| Hierarchical to: | No other components. |
| FAU_STG_EXT.1.1 | The TSF shall be able to transmit the generated audit data to an external IT entity. |
| FAU_STG_EXT.1.2 | The TSF shall allow authorized users to configure log-level thresholds for forwarding audit data to configured external IT entities. |
| Dependencies: | FAU_GEN.1 Audit data generation |

## 6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

# 7 Security Functional Requirements

## 7.1 Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

| Security Function | Security Functional Components |
|---|---|
| Security Audit (FAU) | FAU_ARP.1 Security alarms |
| | FAU_GEN.1 Audit data generation |
| | FAU_GEN.2 User identity association |
| | FAU_SAA.1 Potential violation analysis |
| | FAU_SAR.1 Audit review |
| | FAU_STG_EXT.1 External audit trail storage |
| | FAU_STG.2 Guarantees of audit data availability |
| Cryptographic Support (FCS) | FCS_CKM.1 Cryptographic key generation |
| | FCS_CKM.4 Cryptographic key destruction |
| | FCS_COP.1Cryptographic operation |
| User Data Protection (FDP) | FDP_IFC.1 Subset information control |
| | FDP_IFF.1 Simple security attributes |
| | FDP_RIP.2 Full residual information protection |
| Identification and Authentication (FIA) | FIA_ATD.1 User attribute definition |
| | FIA_UAU.2 User authentication before any action |
| | FIA_UAU.5 Multiple authentication mechanisms |
| | FIA_UAU.7 Protected authentication feedback |
| | FIA_UID.2 User identification before any action |
| | FIA_USB.1 User-subject binding |
| Security Management (FMT) | FMT_MOF.1 Management of security functions behavior |
| | FMT_MTD.1 Management of TSF data |
| | FMT_SMF.1 Specification of management functions |
| | FMT_SMR.1 Security Roles |
| Protection of the TSF (FPT) | FPT_FLS.1 Failure with preservation of secure state |
| | FPT_STM.1 Reliable time stamp |
| | FPT_TST.1(1) TSF Self-Test |
| | FPT_TST.1(2) TSF Self-Test |
| Resource Utilization (FRU) | FRU_FLT.1(1) Fault Tolerance |
| | FRU_FLT.1(2) Fault Tolerance |
| | FRU_PRS.1 Limited priority of service |
| | FRU_RSA.1 Maximum quotas |
| TOE Access (FTA) | FTA_SSL.3 TSF-initiated termination |
| | FTA_SSL.4 User-initiated termination |
| | FTA_TSE.1 TOE session establishment |
| | FTA_TAB.1 Default TOE access banners |
| Trusted Path/Channels (FTP) | FTP_TRP.1 Trusted path |

**Table 7-1: Security Functional Requirements for the TOE**

### 7.1.1 Class FAU: Security Audit

#### 7.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take the following actions: [***send SNMP trap***] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

#### 7.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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 [basic] level of audit; and

c) [***specific events related to FAU_SAA.1: failed authentication, temperature threshold exceeded, fan is no longer operational, port link status up/down, line card(s) are no longer operational, power supply ceased functionality***].

| Component | Event |
|---|---|
| FAU_ARP.1 | Actions taken due to potential security violations |
| FAU_SAA.1 | Enabling and disabling of any of the analysis mechanisms; Automated responses performed by the tool |
| FAU_SAR.1 | Searching audit data |
| FAU_EXT_STG.1 | Sending audit data to the external servers |
| FAU_STG.2 | Actions taken due to exceeding the audit data threshold |
| FIA_UAU.2 | Successful and unsuccessful use of authentication mechanisms |
| FIA_UAU.5 | Successful and unsuccessful use of authentication mechanisms |
| FIA_UAU.7 | Successful and unsuccessful use of authentication mechanisms |
| FIA_UID.2 | Successful and unsuccessful use of authentication mechanisms |
| FIA_USB.1 | Success and failure of binding of user security attributes to a subject |
| FMT_MOF.1 | All modifications in the behavior of the functions in the TSF (See Table 7-3) |
| FMT_MTD.1 | All modifications of the values of TSF data by the administrator (See Table 7-3) |
| FMT_SMF.1 | All use of the management functions (See Table 7-3) |
| FMT_SMR.1 | Modifications of users assigned to a role |
| FPT_FLS.1 | Failure of TOE components |
| FPT_STM.1 | Changes to the time |
| FPT_TST.1(1) | Failure of TOE components |
| FPT_TST.1(2) | Failure of TOE components |
| FTA_SSL.3 | Termination of an interactive session due to user inactivity |
| FTA_SSL.4 | Termination of an interactive session by the user |
| FTP_TRP.1 | All attempted uses of the trusted path functions, Identification of the user associated with all trusted path invocations, if available |

**Table 7-2: 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, [***severity***].

Dependencies: FPT_STM.1 Reliable time stamps

*Application Note:* *The severity is defined as log-level as well as a numerical representation of log-level. Please refer to Section 9.1.1.1 for the full list and descriptions of each severity/log-level.*

#### 7.1.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

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.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

#### 7.1.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [***failed authentication, temperature threshold exceeded, fan is no longer operational, port link status up/down, line card(s) are no longer operational, power supply ceased functionality***] known to indicate a potential security violation;

b) [***no other rules***].

Dependencies: FAU_GEN.1 Audit data generation

#### 7.1.1.5 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [***1. all users, 2. Admin-level or higher users***] with the capability to read [***1. commands below Super-level user commands, 2. all data***] 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.

Dependencies: FAU_GEN.1 Audit data generation

#### 7.1.1.6 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1 Protected audit trail storage

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [***all but the oldest***] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion].

Dependencies: FAU_GEN.1 Audit data generation

#### 7.1.1.7 FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity.

FAU_STG_EXT.1.2 The TSF shall allow authorized users to configure log-level thresholds for forwarding audit data to configured external IT entities.

Dependencies: FAU_GEN.1 Audit data generation

### 7.1.2 Class FCS: Cryptographic Support

#### 7.1.2.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

[***RSA***] and specified cryptographic key sizes [***2048-bit***] that meet the following: [***RFC 3268***].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

#### 7.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***overwrite***] that meets the following: [***no standard***].

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]

#### 7.1.2.3 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***AES***] and cryptographic key sizes [***256-bit***] that meet the following: [***RFC 3268***].

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

### 7.1.3 Class FDP: User Data Protection

#### 7.1.3.1 FDP_IFC.1 Subset Information Control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [***Ciena Carrier Ethernet Flow Control SFP***] on [

- ***subjects: transport service***
- ***objects: network packets***
- ***operations: forward*]**.

*Application Note:* *Transport Service attributes can be composed of a physical port, C-tag, S-tag, PBB/PBB-TE encapsulation (BVID, ISID), and MAC Address.*

Dependencies: FDP_IFF.1 Simple security attributes

#### 7.1.3.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [***Ciena Carrier Ethernet Flow Control SFP***] based on the following types of subject and information security attributes: [***attributes of service: physical port (required), C-tag, S-tag, PBB/PBB-TE encapsulation (BVID, ISID), MAC Address***].

FDP_IFF.1.2 **Refinement:** The TSF shall permit an information flow between a controlled ~~source~~ ***source subject*** and controlled ~~information~~ ***destination subject*** via a controlled operation if the following rules hold: [***the information security attributes within the network traffic match the attributes within a specified service as defined by the Ciena Carrier Ethernet Flow Control SFP***].

FDP_IFF.1.3 The TSF shall enforce the **[following rules**:

- ***ACLs defined within the TOE to deny information flow from specified IP addresses and/or MAC addresses within the ACL;***
- ***Explicitly defined MAC addresses allowed for a specific port are the only MAC addresses allowed to transfer network traffic over a specific port, if applicable;***
- ***MAC learning table for each physical port is limited by a configurable amount of MAC addresses;***
- ***Configurable VLAN number (default 127) redirects network flow traffic to the management plane;***
- ***Customer Premise Equipment must authenticate to the TOE via 802.1x authentication].***

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [***no other rules***].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [***no other rules***].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

#### 7.1.3.3 FDP_RIP.2 Full Residual Information Protection

Hierarchical to: FDP_RIP.1 Subset residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

Dependencies: No dependencies.

### 7.1.4 Class FIA: Identification and Authentication

#### 7.1.4.1 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***username, password, role***].

Dependencies: No dependencies.

*Application Note:* *Vendor documentation specifically refers to roles as "privilege levels."*

#### 7.1.4.2 FIA_UAU.2 User Authentication before Any Action

Hierarchical to: FIA_UAU.1 Timing of authentication

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.

Dependencies: FIA_UID.1 Timing of identification

#### 7.1.4.3 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [***local authentication, RADIUS, TACACS+***] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***global configuration defined by users of the minimum privilege level of "Admin"***].

*Application Note:* *Authorized users are able to enable authentication mechanisms and set an order of precedence. In the event of the first authentication mechanism failing (authentication*

*Services are unable to connect to RADUIS or TACACS servers), then the authentication mechanism next in the line of precedence is deferred to.*

Dependencies: No dependencies.

#### 7.1.4.4 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [***obscured password display, simple "failed to authenticate" messages***] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

#### 7.1.4.5 FIA_UID.2 User Identification before Any Action

Hierarchical to: FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies.

#### 7.1.4.6 FIA_USB.1 User-Subject Binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***all user attributes as specified in FIA_ATD.1***].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***association of a user's attributes to a session object***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***Revocation of the user-subject binding and termination of the user's session under the following conditions: user logging out, user being logged out due to inactivity***].

Dependencies: FIA_ATD.1 User attribute definition

### 7.1.5 Class FMT: Security Management

#### 7.1.5.1 FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, modify the behavior of] the functions [***Ciena Carrier Ethernet Suite Flow Control SFP***] to [***Super, and Admin roles***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

#### 7.1.5.2 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, [***operations in Management Activities column of Table 7-3***]] the [***objects found within Management Activities in Table 7-3***] to [***the minimum authorized role as defined in Table 7-3***].

*Application Note:* *The privilege levels in the last column of Table 7-3 are the minimum privilege levels required for the corresponding management activities. The management activities available to each privilege level are also available to all privilege levels higher than the one specified.*

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

#### 7.1.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***list of management functions in Table 7-3***].

| Requirement | Management Activities | Minimum Privilege Level Required |
|---|---|---|
| FAU_ARP.1 | Management of actions to be taken when alert is triggered | Admin |
| FAU_SAA.1 | Management of rules which cause alert to be triggered | Admin |
| FAU_SAR.1 | Management of users who have read access to audit records | N/A – users have read access to audit records pertinent to their role. |
| FAU_STG.2 | Maintenance of parameters which govern audit storage | N/A |

| | | |
|---|---|---|
| FAU_STG_EXT.1 | Management of external audit storage location through configuration of the syslog collector and log-level threshold | Admin |
| FDP_IFF.1 | Management of attributes used to make information flow decisions | Admin |
| FIA_UAU.2 | Management of authentication data | Super |
| FIA_UAU.5 | Management of authentication mechanisms and rules for authentication | Admin |
| FIA_UID.2 | Management of user identities | Super |
| FIA_USB.1 | Management of subject security attributes | Super |
| FMT_MOF.1 | Management of roles that can interact with the TSF | N/A - roles are statically defined |
| FMT_MTD.1 | Management of roles that can interact with TSF data | N/A - roles are statically defined |
| FMT_SMR.1 | Management of users who belong to a specified role | Super |
| FPT_STM.1 | Management of system time | Admin |
| FRU_PRS.1 | Assignment of priorities to subject usage of resources | Admin |
| FRU_RSA.1 | Maximum limits for subject usage of resources | Admin |
| FTA_SSL.3 | Specification of timeout duration | Admin |
| FTA_TAB.1 | Specification of banner text | Admin |
| FTA_TSE.1 | Management of session establishment conditions | N/A - session establishment denial is based on fixed maximum number of concurrent sessions |
| FTP_TRP.1 | Configuration of actions which require use of trusted path | Admin |

**Table 7-3: Management Activities**

Dependencies: No dependencies.

*Application Note:* *The "Admin" role does not exist in SDS machines. All "Admin" references in this table can be viewed as "Super" for SDS models.*

#### 7.1.5.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***Super, Admin, and Limited***].

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

*Application Note:* *Limited user is read-only. Admin user can read and make configuration changes, excluding users. Super user can read and make configuration changes, including changes to users.*

Dependencies: FIA_UID.1 Timing of identification

### 7.1.6 Class FPT: Protection of the TSF

#### 7.1.6.1 FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- ***Control Card fails within a chassis-based TOE***
- ***Service link is broken within a system with redundant physical links***

].

Dependencies: No dependencies.

#### 7.1.6.2 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies.

#### 7.1.6.3 FPT_TST.1(1) TSF Self-Test

Hierarchical to: No other components.

FPT_TST.1.1(1) The TSF shall run a suite of self tests [during initial start-up], to demonstrate the correct operation of [the TSF].

FPT_TST.1.2(1) The TSF shall provide authorised users with the capability to verify the integrity of [***none***].

FPT_TST.1.3(1) The TSF shall provide authorised users with the capability to verify the integrity of [***CPU register and memory space***].

Dependencies: No dependencies.

#### 7.1.6.4 FPT_TST.1(2) TSF Self-Test

Hierarchical to: No other components.

FPT_TST.1.1(2) The TSF shall run a suite of self tests [***between Control Cards and line cards upon Control Card failover***] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2(2) The TSF shall provide authorised users with the capability to verify the integrity of [***TOE configuration data***].

FPT_TST.1.3(2) The TSF shall provide authorised users with the capability to verify the integrity of [***none***].

Dependencies: No dependencies.

### 7.1.7 Class FRU: Resource Utilization

#### 7.1.7.1 FRU_FLT.1(1) Fault Tolerance

Hierarchical to: No other components.

FRU_FLT.1.1(1) The TSF shall ensure the operation of [***control plane functionality***] when the following failures occur: [***a single Control Card fails within a chassis-based TOE***].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

#### 7.1.7.2 FRU_FLT.1(2) Fault Tolerance

Hierarchical to: No other components.

FRU_FLT.1.1(2) The TSF shall ensure the operation of [***data flow functionality***] when the following failures occur: [***a service link is broken within a system with redundant physical links***].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

#### 7.1.7.3 FRU_PRS.1 Limited Priority of Service

Hierarchical to: No other components.

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

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

Dependencies: No dependencies.

#### 7.1.7.4 FRU_RSA.1 Maximum Quotas

Hierarchical to: No other components.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [***bandwidth***] that [***subjects***] can use [***simultaneously***].

Dependencies: No dependencies.

### 7.1.8 Class FTA: TOE Access

#### 7.1.8.1 FTA_SSL.3 TSF-Initiated Termination

Hierarchical to: No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [***authorized user-configurable amount of time***].

Dependencies: No dependencies.

#### 7.1.8.2 FTA_SSL.4 User-Initiated Termination

Hierarchical to: No other components.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

Dependencies: No dependencies.

#### 7.1.8.3 FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [***Number of concurrent sessions total and by role (Admin-configurable):***

- ***Limited: 0-9 maximum;***
- ***Admin: 0-9 maximum;***
- ***Super: 0-9 maximum;***
- ***SSH Sessions: 15 maximum***].

Dependencies: No dependencies.

*Application Note:* *The 15 maximum SSH sessions is a static value on the SAOS 7.x devices and cannot be configured. For SAOS 6.x devices, the maximum number of simultaneous SSH sessions is not statically configured and is instead limited to 15 by the device's performance.*

#### 7.1.8.4 FTA_TAB.1 Default TOE Access Banners

Hierarchical to: No other components.

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

Dependencies: No dependencies.

### 7.1.9 Class FTP: Trusted Path/Channels

#### 7.1.9.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

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, [***all user management functions***]].

Dependencies: No dependencies.

## 7.2 Operations Defined

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were modified from existing Security Audit (FAU) requirements, are designed to address the requirements for the TOE's primary function, which is Carrier Ethernet switching.

The CC permits four functional component operations—assignment, refinement, selection, and iteration —to be performed on functional requirements. This ST will highlight the four operations in the following manner:

- Assignment: allows the specification of an identified parameter. Indicated with ***bold text and italics*** if further operations are necessary by the Security Target author.
- Refinement: allows the addition of details. Indicated with ***underlined bold text and italics*** if further operations are necessary by the Security Target author.
- Selection: allows the specification of one or more elements from a list. Indicated with underlined text.

- Iteration: allows a component to be used more than once with varying operations. Indicated with the iteration number within parentheses after the short family name, e.g. FAU_GEN.1 (1), FAU_GEN.1 (2).

# 8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2.

## 8.1 Security Architecture

### 8.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D: The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D: The developer shall design and implement the TSF so that it is able to protect itself from tampering by un-trusted active entities.

ADV_ARC.1.3D: The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C: The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C: The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C: The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C: The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 8.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1D: The developer shall provide a functional specification.

ADV_FSP.2.2D: The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C: The functional specification shall completely represent the TSF.

ADV_FSP.2.2C: The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C: The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C: For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C: For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C: The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E: The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

### 8.1.3 Basic Design (ADV_TDS.1)

ADV_TDS.1.1D: The developer shall provide the design of the TOE.

ADV_TDS.1.2D: The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C: The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C: The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C: The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C: The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C: The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C: The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

ADV_TDS.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E: The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

## 8.2 Guidance Documents

### 8.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 8.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of

the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator *shall apply* the preparative procedures to confirm that the TOE can be prepared securely for operation.

## 8.3 Lifecycle Support

### 8.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1D: The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D: The developer shall provide the CM documentation.

ALC_CMC.2.3D: The developer shall use a CM system. ALC_CMC.2.1C: The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C: The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 8.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1D: The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 8.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## 8.4 Security Target Evaluation

### 8.4.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

### 8.4.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

| | |
|---|---|
| ASE_ECD.1.1C | The statement of security requirements shall identify all extended security requirements. |
| ASE_ECD.1.2C | The extended components definition shall define an extended component for each extended security requirement. |
| ASE_ECD.1.3C | The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes. |
| ASE_ECD.1.4C | The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation. |
| ASE_ECD.1.5C | The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated. |
| ASE_ECD.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| ASE_ECD.1.2E | The evaluator shall confirm that no extended component can be clearly expressed using existing components. |

### 8.4.3 ST Introduction (ASE_INT.1)

| | |
|---|---|
| ASE_INT.1.1D | The developer shall provide an ST introduction. |
| ASE_INT.1.1C | The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description. |
| ASE_INT.1.2C | The ST reference shall uniquely identify the ST. |
| ASE_INT.1.3C | The TOE reference shall identify the TOE. |
| ASE_INT.1.4C | The TOE overview shall summarize the usage and major security features of the TOE. |
| ASE_INT.1.5C | The TOE overview shall identify the TOE type. |
| ASE_INT.1.6C | The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE. |
| ASE_INT.1.7C | The TOE description shall describe the physical scope of the TOE. |
| ASE_INT.1.8C | The TOE description shall describe the logical scope of the TOE. |
| ASE_INT.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

### 8.4.4 Security objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 8.4.5 Derived security requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirement's rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

| | |
|---|---|
| ASE_REQ.2.5C | Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied. |
| ASE_REQ.2.6C | The security requirements rationale shall trace each SFR back to the security objectives for the TOE. |
| ASE_REQ.2.7C | The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE. |
| ASE_REQ.2.8C | The security requirements rationale shall explain why the SARs were chosen. |
| ASE_REQ.2.9C | The statement of security requirements shall be internally consistent. |
| ASE_REQ.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### 8.4.6 Security Problem Definition (ASE_SPD.1)

| | |
|---|---|
| ASE_SPD.1.1D | The developer shall provide a security problem definition. |
| ASE_SPD.1.1C | The security problem definition shall describe the threats. |
| ASE_SPD.1.2C | All threats shall be described in terms of a threat agent, an asset, and an adverse action. |
| ASE_SPD.1.3C | The security problem definition shall describe the OSPs. |
| ASE_SPD.1.4C | The security problem definition shall describe the assumptions about the operational environment of the TOE. |
| ASE_SPD.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### 8.4.7 TOE Summary Specification (ASE_TSS.1)

| | |
|---|---|
| ASE_TSS.1.1D | The developer shall provide a TOE summary specification. |
| ASE_TSS.1.1C | The TOE summary specification shall describe how the TOE meets each SFR. |
| ASE_TSS.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| ASE_TSS.1.2E | The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description. |

## 8.5 Tests

### 8.5.1 Evidence of Coverage (ATE_COV.1)

| | |
|---|---|
| ATE_COV.1.1D: | The developer shall provide evidence of the test coverage. |
| ATE_COV.1.1C: | The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification. |
| ATE_COV.1.1E: | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### 8.5.2 Functional Testing (ATE_FUN.1)

| | |
|---|---|
| ATE_FUN.1.1D | The developer shall test the TSF and document the results. |
| ATE_FUN.1.2D | The developer shall provide test documentation |
| ATE_FUN.1.1C | The test documentation shall consist of test plans, expected test results and actual test results. |
| ATE_FUN.1.2C | The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests. |
| ATE_FUN.1.3C | The expected test results shall show the anticipated outputs from a successful execution of the tests. |
| ATE_FUN.1.4C | The actual test results shall be consistent with the expected test results. |
| ATE_FUN.1.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |

### 8.5.3 Independent Testing - Sample (ATE_IND.2)

| | |
|---|---|
| ATE_IND.2.1D | The developer shall provide the TOE for testing. |
| ATE_IND.2.1C | The TOE shall be suitable for testing. |
| ATE_IND.2.2C | The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. |
| ATE_IND.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| ATE_IND.2.2E | The evaluator shall execute a sample of tests in the test documentation to verify the developer test results. |
| ATE_IND.2.3E | The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified. |

## 8.6 Vulnerability Assessment

### 8.6.1 Vulnerability Analysis (AVA_VAN.2)

| | |
|---|---|
| AVA_VAN.2.1D | The developer shall provide the TOE for testing. |
| AVA_VAN.2.1C | The TOE shall be suitable for testing. |
| AVA_VAN.2.1E | The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. |
| AVA_VAN.2.2E | The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE. |
| AVA_VAN.2.3E | The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE. |
| AVA_VAN.2.4E | The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. |

# 9 TOE Summary Specification

## 9.1 TOE Security Functions

The following sections identify the security functions of the TOE. They include Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access, and Trusted Path/Channels.

### 9.1.1 Security Audit

The TOE supports audit generation in the form of syslogs. All user actions performed on the TOE are logged. Some general classifications of these user actions can be configuring the flow control policy, configuring users and authentication. The full list of auditable events is defined in Table 7-2 Auditable Events.

#### 9.1.1.1 Syslog

The TOE has the ability to log every event locally and remotely. Syslog messages are sent from the TOE to the syslog server. These messages are not encrypted. The user can specify the severity for which syslog messages are sent over to the collector. Each event generated by the TOE has a severity associated with it. The user may configure the TOE to only transmit messages greater than or equal to the minimum severity and less than or equal to the maximum severity. The TOE has eight defined event severity settings: Critical, Major, Minor, Warning, Informational, Debug, Cleared, and Config. The following table describes the severity settings:

| Event Severity (Syslog Severity Value) | Definition |
|---|---|
| Critical (0) | Indicates that there is a condition in the TOE that affects the service of the switch. This type of event requires immediate corrective action, as it may affect multiple subscribers of the switch. |
| Major (1) | Indicates that there is a condition in the switch that requires urgent corrective action. "Major" messages are also service-affecting, but only affect a very small number of services. |
| Minor (3) | Indicates that there exists a non-service affecting fault condition. Corrective action should be taken in order to prevent a more serious fault within the TOE. |
| Warning (4) | Indicates that there was a detection of a potential service affecting fault before any significant effects have occurred on the TOE. Action should be taken to correct the problem before it becomes a more serious fault. |
| Informational (7) | Indicates that there is an occurrence on the device that is not associated with TOE performance degradation. No action is required by the user. |
| Debug (7) | Indicates a class of events that are not intended for normal operation of the TOE and are only used for troubleshooting. In general, "debug" messages are filtered. |

| | |
|---|---|
| Cleared (7) | Indicates that a previous reported alarm is now cleared. The "cleared" severity overrules the previous severity setting. |
| Config (5) | Indicates a configuration change. This syslog message is primarily used for communicating the system configuration changes to the TOE's internal interfaces and external entities. |

**Table 9-1: Event and Syslog Severity**

Critical events require low severity values, while less severe events have higher values.

Each syslog record contains the date and time, severity, user, and message about the event. The TOE provides the syslog record in the following format: <day> <year> <date-time>: <severity> <id string> <message string>. The "id string" field displays the user IP address, while the "message string" field displays a short summary of the user actions. The following is an example of a logged event for the Admin user enabling a port on the TOE:

"January 28, 2011 22:55:05.741 [local] Sev:7 chassis(1)Telnet IP 127.0.0.1 User admin:Port Enable port 5/3 enabled"

#### 9.1.1.1.1 Syslog Configuration

The TOE provides the functionality to configure the syslog collectors. Syslog servers can be configured using DHCP by those users with, at minimum, Admin privileges. These authorized users can add/remove syslog collectors, add severity levels, create/delete a collector, enable/disable a collector, and configure collectors. For instance, the command "syslog add collector 192.168.10.63 severity critical" would allow the transmission of audits at the specified severity level "critical" to the specified collector.

For each syslog collector, an authorized user can configure the collected logs, the syslog message prefix, syslog facility, and UDP port (default is 514). With these commands and "set syslog," an Admin user or Super user can configure the default settings for any syslog created thereafter.

### 9.1.1.2 Command Log

The command log records every TOE command from the CLI. All user actions initiated from the CLI are audited. The command log contains information as to the success or failure of the event, as well as the role and user associated with the action. The command log contains the records of a user's CLI authentication and management functions. The log details the user, role, network identifiers, time, command string, and the result of the command for each event.

The TOE provides the capability to view this log with the "command-log show" command. All users can view the command log, but Limited users cannot view commands that require Super user or above access. Users with the minimum Admin-level privilege are able to delete the logs, but the TOE does not allow any user to have the capability to modify the audit log information.

The TOE allocates four files for logging events. When one file reaches the maximum size, the next file is used to store the logs. When all four log files have reached the maximum capacity for data, the oldest file becomes the newest file to be overwritten with current log information. The size of the log files depends on the device platform. The 3930 and 5150 series devices have 32 MB allocated for log files. The 5305 and 5410 series models limit the log file sizes differently for each log. Details on the specific restrictions on log files for the 5305 and 5410 devices are as follows:

- 5305
  - Command log – holds a maximum of 2,000 records
  - Fault log – holds a maximum of 900,000 records
  - syslog – has a maximum size of 4MB
- 5410
  - Command log – holds a maximum of 10,000 records
  - Event log – holds a maximum of 3,000 records
  - Fault log – holds a maximum of 900,000 records
  - syslog – has a maximum size of 4MB

The following is an example of a recorded command log event:

"Fri Jan 28 22:51:32 2011 | admin(admin) /telnet_127.0.0.1:41228 | port enable port 5/3"

#### 9.1.1.3 Alarms and Events

The TOE monitors for potential security violations or error conditions in the events that get audited. The TOE allows for specific types of failures to generate alerts. The events are as follows: failed authentication occurs, the temperature threshold has been exceeded, a fan is no longer operational, port link status is up or down, line card(s) are no longer operational, and a power supply has ceased functionality. The TOE generates an audit log for each of these failure conditions. The TOE will trigger an alarm condition based on the audit log if any of the conditions occur.

TOE faults are detected when the system becomes aware of a failure causing a loss of service. Faults are handled by the fault manager to protect the system hardware from potential damage. Fault alarms are registered throughout the TOE as SNMP traps and system log messages. SNMP traps are sent to the SNMP Manager. The TOE uses SNMP v3.

The types of events that trigger SNMP traps are not limited to alarms. SNMP traps may be sent out based on a configured set of events. This set of events is a subset of those that can trigger syslog messages. However, the SNMP and Syslog related internal components are independent.

### 9.1.2 Cryptographic Support

Secure Shell (SSH) provides secure access to remote systems. SSH verifies and grants access to log in requests by encrypting user ID and passwords for authentication. Once an SSH session is established all subsequent traffic over the session is sent in encrypted

form as well. This effectively makes SSH a functionally equivalent, but secure version of Telnet. All cryptographic functionality implemented within the TOE is not validated by FIPS 140-2, but is asserted to be accurate by the vendor.

To ensure secure communication through the user sessions, the TOE requires a user to authenticate through an SSH connection. All telnet sessions have been disabled without the use of an SSH version 2 (v2) client. The SSH authentication generates a public and private key pair using the "ssh-keygen" utility to create the 2048-bit RSA key when the user initiates with the TOE. In this public key based authentication, the key pair is generated, then encrypted and stored on the server. If the key has already been generated, the command "ssh server key generate" will fail with the error: "ERROR: Key already exists." All users of the minimum Admin privilege level can delete the key by issuing the command "ssh server key delete" and then generate the key with the key generation command. The key delete command deletes the key, and overwrites the data sector with pseudo-randomly generated data. This prevents the possibility of viewing the residual information of the cryptographic data.

All connections to the TOE connect to the SSH server, generating an SSH session. Upon having an SSH session established, users must identify and authenticate themselves to the TOE to create a CLI session. All data sent within the TOE's subsystems to the CLI through SSH is encrypted throughout the transit. Within this trusted channel, the TOE uses 256-AES encryption. All SNMP traffic transferred between the TOE and an SNMP Manager is encrypted using standard SNMPv3 cryptographic methods. All files sent to an SFTP client contain encryption on the user ID, password and file contents, while the file is transferred over the SSH server listener port. This last transmission only occurs during initialization and is not used during regular runtime of the TOE.

For local authentication, the TOE checks against internally stored user data versus the inputted username and password to grant or deny user access. The password data is hashed using MD5 and all inputted password data during authentication is also hashed using the same mechanism.

When authenticating to the TOE via telnet through SSH, the TOE sends authentication requests to the RADIUS server. The server keeps track of all user authentication and service access information. The RADIUS server also returns these authentication results to the TOE, and each user will either be allowed or denied access based on the information from the server. The RADIUS server contains a pre-shared key which is the authentication string used to verify that the TOE is authorized to access the RADIUS server. The key must be between 8 and 128 characters in length and must be the same for all RADIUS servers specified.

The TACACS+ protocol client is supported where the device operates as a NAS. TACACS+ grants access to users when the user first logs in to the TOE. TACACS+ also provides additional security by using a pre-shared key to encrypt information between the TOE and the authentication server. The key must be between 8 and 64 characters in length and must be the same for all TACACS+.

### 9.1.3 User Data Protection

The core functionality of the TOE is to perform Carrier Ethernet functionality to a network. This entails defining services from traffic header information and prioritizing, scheduling, and forwarding services to physical ports. CES devices are capable of handling untagged, VLAN tagged and PBB frames. The TOE uses CoS and QoS to provision the frames on a by-service level. In addition, any Customer Premise Equipment (CPE) connected to the TOE must authenticate to the TOE via 802.1x authentication. The TOE provides ingress and egress processing of data. The ingress frames from which the virtual switch resolves to are determined by the internal interfaces on the TOE because it is a Layer 2 device. The TOE internally processes ingress frames and forwards the traffic to specific egress ports based on the services associated with the traffic frames. The TOE does not explicitly authorize or deny other than the internal processing of the service attributes, ACLs, and MAC learning tables used to determine the egress ports to which the ingress ports will be forwarded.

The TOE can either be a Service Delivery Switch (SDS) or a Service Aggregation Switch (SAS). Both types of switches are functionally identical, with the only difference between them being performance-based. SDS's are intended to be deployed on the edge of a network where host devices are able to directly connect to the switch. SAS's are intended to be deployed in the core or backbone of a network, as they are designed to handle high levels of throughput.

#### 9.1.3.1 Service Attributes

The TOE contains physical ports, sub-ports, PBB-TE tunnels, PBB-TE tunnel groups, a PBB-TE service interface, and a PBB-TE transit interface. The C-tag and S-tag are contained in the VLAN headers. The TOE's forwarding depends on the S-Tag and destination MAC address. The BVID and ISID are attributes within PBB-TE. These attributes of transport service can be used when creating attributes to associate network frames with logical services. Physical ports refer to the physical port number on the appliance itself. These ports allow external devices to physically connect to the TOE. The source MAC address is the MAC address of the source device, and remains associated with the traffic throughout transit. The destination MAC address is the MAC address to which the frames will be forwarded. Each frame's security attributes aid in determining the destination of the forward.

#### 9.1.3.2 Access Control Lists

Each frame is also compared to an IP Access Control List (IP-ACL). The IP-ACL defines the IP combinations that are allowed to communicate with the device. Frames containing items that do not match any configured ACL entry will be discarded. The ACL compares the IP source address and ingress port number with the ACL entries. The ACLs on the TOE prevent unauthorized IP address from communicating with the TOE. The 7.x version of the TOE also allows MAC addresses to be contained in the ACL entries in order to explicitly permit and/or deny traffic coming in from a specific port on the TOE.

#### 9.1.3.3 MAC Learning

The TOE is capable of MAC learning, which allows the Ethernet switch to identify the MAC addresses of traffic with regard to the port the traffic is sent. Therefore, the forwarding depends on the MAC address of the traffic frames. Ingress traffic on a physical port is forwarded to other sub-ports. These additional sub-ports are connected to physical ports where the data will aggregate out from. Once this occurs, the MAC tables are updated and the TOE learns the associations for those data frames. The TOE then uses MAC forwarding to send the frame out based on the MAC learning process, in which the TOE remembers port information associated with each device connected to a physical port on the TOE. The TOE can then prevent MAC address explosion and MAC flooding by limiting the number of MAC addresses learned on each port. This prevents an overflow of MAC addresses within the CAM table, where MAC addresses are stored.

#### 9.1.3.4 Traffic Flow

The traffic flow is also determined by the port association, ingress rules and egress rules for acceptable frame types. Each frame type is checked to determine the tag on the frames arriving at a port on the TOE. Each port on the TOE has an associated Acceptable Frame Type parameter that determines if the port accepts or denies untagged frames. All tagged frames are further processed based on the ingress rules set on the port. Traffic entering on the Data Plane that is set for the Management Plane will be forwarded internally to the Management Plane instead of being forwarded through the normal switching functionality. It will not be put into normal forwarding domains, so that the traffic can be directed from the Data Plane to the Management Plane. Users must use SSH to connect to the CLI through this method similarly to the normal local Ethernet management connection. The difference is the local Ethernet management connection is out-of-band from the normal switch traffic. The TOE can also direct network traffic to the management plane through configuring the VLAN number of the traffic. The default VLAN number is 127.

#### 9.1.3.5 Residual Data

Data that is stored in memory has full residual protection through the use of overwrite and Zeroization mechanisms. Once a user session is terminated or an object no longer needs data stored in a part of memory, the TOE will perform two possible actions. First, the TOE may zeroize all the data using internal functionality. Alternatively, the TOE may overwrite the old values with new values based upon actions from new user sessions.

### 9.1.4 Identification and Authentication

The TOE provides one interface to log on to the system in the evaluated configuration: the command line interface (CLI) through an SSH connection. Users can connect to the TOE through an Ethernet connection on the Ethernet Management Port or through remote access. If a remote user attempts a Telnet connection without authenticating via SSH, the user will be denied access to the TOE. All user authentication and user management

must occur over the SSH session. The users must identify and authenticate before any other actions can occur on the TOE.

#### 9.1.4.1 User attributes

Each user has the following security attributes associated with them:

- User name
- Password
- Role (privilege level)

The user name and password are for authenticating to the TOE. The role can be Limited, Admin, or Super, depending on the role assigned to by a user of privilege level "Super".

#### 9.1.4.2 Authentication Methods

The TOE provides multiple authentication methods. The TOE can support local authentication with user name and password, RADIUS, and TACACS+. When a user accesses the CLI through the SSH connection, the TOE requests a username and password. When entering passwords, the TOE only displays obscured text, such that the password characters are never displayed back to the user. With TACACS+ authentication, the TOE does not display or send the password in clear text and after a user is successfully authenticated, the user privilege level is retrieved from the TACACS+ server.

RADIUS also provides remote authentication, but works slightly differently. When authenticating via RADIUS, the TOE sends the requests to the RADIUS server. User roles are stored in the RADIUS server and are not mapped to privilege levels as they are in TACACS+ servers. The roles are defined through the use of Vendor-Specific Attributes (VSAs). The RADIUS server checks the users' privileges with the role associated with the authenticated users. This server keeps a log of all user authentication and service access information. The user will be granted or denied access based on the records sent from the servers to the TOE.

The TOE does not allow any TSF-mediated actions before the user is identified and authenticated. After authentication, the user's security attributes are associated with the user subjects. Session objects are created for TOE sessions, each containing the unique process ID for the CLI process used and the user name and user role mapped to the authenticated user. Once the authentication occurs, the role information from the external authentication servers is associated with the user on the TOE for that user session. The TOE's authorization information is used in creating sessions and session objects. This includes changes to security attributes associated with the user subjects, such that the updates are reflected appropriately. If a user logs out using the "quit" command, that user's session is ended immediately. Additionally, if a user is inactive for an Admin-configurable amount of time, the session will be disconnected by the TOE itself. When a

user account is deleted, the TOE removes both the account and its assigned role. Once this has been performed, no logon attempt by the deleted user will be successful.

Upon authentication failure, the TOE will display a message to the user stating that the login is incorrect. In the event of a failed authentication attempt, the CLI will not vary output messages. Whether or not the username is valid, the response message does not change. If a user's password is forgotten, it cannot be retrieved. A new password would need to be assigned by an authorized user. All user information is saved in the Security Config section of the configuration file, but the password is encrypted and saved with the attribute of secret.

#### 9.1.4.3 Authentication Order

By default, the TOE queries its local database for user authentication. It is possible however to configure the TOE so that it leverages backup authentication mechanisms via RADIUS or TACACS+. This can be configured, for example, with the following commands:

1. user auth set order tacacs, radius, local
2. user auth set method tacacs scope remote
3. user auth set method radius scope remote
4. user auth set method local scope serial

With the use of the aforementioned commands, the authentication methods have been placed into a hierarchical structure. The TOE will check TACACS+ for authentication credentials for a user unless it cannot access the server. If this were to occur, configuration would automatically direct the authentication request to RADIUS. The scope statement at the end of the last three commands also provides the purpose of separating how authentication is performed from a remote or serial interface, or both. The order in which the TOE checks the different authentication mechanisms corresponds to the order the mechanisms are listed in the "set order" command. For the aforementioned example, TACACS+ would handle remote authentication first followed by RADIUS. The local database would only handle local authentication attempts through the serial port.

To confirm that the hierarchical structure has been configured correctly, the command "user auth show" will display the priority, scope, and activity of each authentication method.

### 9.1.5 Security Management

The TOE enforces security management through the roles defined within the TOE. Each role has different levels of authorization in terms of the functions that can be performed by the users of the respective role. The default role for a user is set to Limited, which lacks the privileges to make configuration changes to the TOE. All users on the TOE must have exactly one role assigned to their user account.

#### 9.1.5.1 Roles

Users of the TOE can be assigned to three different roles, Limited, Admin, and Super. Each user is assigned to a role upon the creation of the account. Users are referred to the role in which the user is associated with, i.e. a user with a Limited role is referenced as a Limited user.

- **Limited user**: A user that is able to execute show commands that do not change the state of the system in a significant way or change the configuration of the device.
- **Admin user**: A user that has all the privileges of the Limited and Admin User and can make significant system state changes, modify the device configuration, and perform execute commands.
- **Super user:** A user that has all the privileges of the Limited and Admin User and can make changes to TOE users and the authentication policy.

Note: the TACACS+ server determines which actions the user is allowed to perform on the TOE based on the role associated with the user ID.

#### 9.1.5.2 Data Management

Those users with the Admin or Super role can perform management of the configuration data on the TOE as well as to user data. As shown in Table 7-3 in Section 7.1.5.4, any user with at least the role of Admin can perform the following management activities:

- Configure the Flow Control Policy
- Configure alert rules
- Create, manage, or delete syslog collectors
- Configure authentication mechanisms and hierarchical structure for authentication
- Manage system time
- Configure telnet session limits for roles
- Configure timeout duration
- Configure default banner
- Configure requirements for trusted path communication

In addition to the following capabilities, those users with the role of Admin can perform management on user roles and authentication data.

### 9.1.6 Protection of the TSF

The TOE connects to an NTP server to ensure accurate time-stamping of response frames. If an NTP server is being used, the TOE automatically synchronizes its time and date to the server which runs on Coordinated Universal Time (UTC). The date and time configuration received from the NTP server overrides any manually set values on the TOE. To prevent an unwanted network intruder from masquerading as an NTP server, HMAC-MD5 message authentication is configured with the NTP client. The authentication method uses keys that are encrypted on both the server and client side, but are used to identify the NTP time server. The time information must be kept as

accurately as possible to correctly apply to the audit information recorded in the event and command log files.

In the event of a service link going down, the TOE can perform one or both of the following: publish an event to the Events and Alarms subsystem or instruct the Data Plane to failover to an active link by switching service links. In the event of a physical port failure, the TOE will notice the failure and publish an event to the Events and Alarms subsystem. The TOE will failover to a secondary port once the primary port link fails. The failover capability allows the TOE to maintain a functional state in the event of failures on the TOE.

The TOE implements two types of self-tests: Power-On Self-Test (POSTs) and conditional self-tests. A POST is invoked once the TOE is powered on, while the conditional self-tests are invoked only when a Control Card fails. The tests are described in greater detail in the following paragraphs.

Upon the startup of the TOE, multiple Power-On Self Tests (POSTs) are run. The POSTs provide environmental monitoring of the TOE's components, in which early warnings can prevent whole component failure. POSTs provide monitoring on the hardware functionality of the TOE such as the CPU registers and memory space. The TOE does not allow users to verify additional functionality other than the TOE configuration data, CPU register and memory space information and gathered during the POSTs.

In the event of a Control Card failing in a chassis-based TOE, the TOE has some capability to remain in a secure state and continue providing functionality in that functional area. The TOE will first perform a conditional self-test, which is also performed on start-up, in which it verifies that the backup control card's configuration is up to date. To perform this verification, the TOE maintains configuration information pertinent to Control Cards. The test will pass once the TOE verifies that the secondary or backup Control Card contains the appropriate and up to date configuration. The roll-over to the backup card will then occur and the backup card will assume Control Card functionality.

### 9.1.7 Resource Utilization

The TOE also has CFM capabilities which serve as fault tolerance. The CFM will continuously monitor performance of its subsystems as well as checking for faults. The CFM also monitors the end-to-end network connectivity of a network service. Services are identified by a Service Instance also known as Service Access Points (SAPs). The TOE maintains two types of SAPs: MEPs and MIPs. MEPs are created at the edge (entry/exit) points, while MIPs are created between the MEPs to track faults at the intermediate points. These methods allow the TOE to be aware of any loss of service at the exact point the service was disrupted. CFM provides the following utilities for the TOE:

- **Path discovery**: MEP transmits multicast frames known as linktrace message which determine the path taken to a target MAC address.
- **Fault detection**: detects connectivity failures and unintended connectivity between services.
- **Fault verification and isolation**: loopback messages confirm successful initiation or restoration of connectivity. Loopback and linktrace messages isolate system faults.
- **Fault notification**: MEP detects the connectivity fault and provides notification of the failure of the associated MEP.
- **Fault recovery:** all fault notifications help network operators correct the errors and replace failed TOE components.

The TOE also maintains fault tolerance when the Control Card on the TOE fails. If this failure occurs the TOE's secondary Control Card will assume the functionality of the primary card. This feature is handled by the redundancy scheme in the hardware. The TOE maintains detection and remediation methods during operation. The hardware will detect the faults and failures, and triggers the software to take action to correct the event.

The TOE assigns priority to the frame and to the service. Higher priority services have less delay time on the TOE. Services with low delay times are less likely to be dropped. The TOE's bandwidth assignment is done by traffic profiling. Traffic profiling classifies ingress traffic based on the Committed and Peak Information Rates, CIR and PIR respectively. These values serve as critical attributes for congestion management throughout the TOE's forwarding process. The TOE's QoS guarantees the minimum and maximum bandwidths for any service on the TOE. PBB-TE specifies the path that the frame traffic will take over the network. PBB-TE provides provisioned QoS metrics by reserving appropriate bandwidth for each frame. The TOE assigns inner tag priority for scheduling frames when the mapping applies to ports associated with PBB-TE tunnels. PBB-TE allows the TOE user to target maximum utilization of the network devices through the use of the PBB queue and queue tag encapsulation. The TOE also allows for frame traffic to be provisioned on a by-service level. Traffic can be designated for use or it can be reserved to a mirror port.

### 9.1.8 TOE Access

The TOE allows users with at minimum "Admin" level privileges to create logon and welcome banner text files to display when SSH sessions are established. However, the default banner for SSH connections to the TOE is set to display "Welcome to the shell" upon authenticating the user and granting access to the TOE. An authorized user must re-configure the banner to state the terms and warnings of use for the TOE in its evaluated configuration.

The TOE also allows any user to initiate the termination of the user session by issuing the "quit" command. Additionally, if a user has not performed any action on the TOE, the

user is termed to be inactive. An inactive user will be disconnected from the TOE if that period of inactivity has reached the Admin-configurable amount of time.

The TOE is able to deny user sessions, as the TOE has a maximum number of concurrent session limits for each role which can be configured by a user with Admin-level privileges or higher. The default TOE limits for SAOS 7.x are as follows:

- No more than 9 Limited users can be logged on to the TOE simultaneously.
- No more than 9 Admin users can be logged on to the TOE simultaneously.
- No more than 9 Super users can be logged on to the TOE simultaneously.
- No more than 15 SSH sessions may be established in parallel.

For SAOS 6.x, there is no hard cap on the number of SSH sessions which may be established, but it is recommended that more than 15 simultaneous sessions be avoided for performance purposes. When more than 8 sessions are active, a warning message will be displayed at the login prompt to make the user aware of the performance impact.

### 9.1.9 Trusted Path/Channels

The TOE provides two user facing communication paths in the evaluated configuration, an Ethernet direct connection to the CLI and a remote terminal session. Both of these communication paths are performed through a CLI with only one difference. The management port is out-of-band traffic while the data plane is in-band traffic through a specific VLAN (default is 127).

The trusted communication path for both interfaces is initiated by the user establishing an SSH connection. SSH provides encryption to protect the communication between the TOE and the users. When an SSH session is generated, the TOE uses an AES 256-bit key to encrypt and decrypt information being sent over the path. This trusted path connection is used from the initial authentication to all management functions that a user attempts to perform through the interfaces.

## 9.2 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

| Security Function | Security Functional Components |
|---|---|
| Security Audit (FAU) | FAU_ARP.1 Security alarms |
| | FAU_GEN.1 Audit data generation |
| | FAU_GEN.2 User identity association |
| | FAU_SAA.1 Potential violation analysis |
| | FAU_SAR.1 Audit review |
| | FAU_STG.2 Guarantees of audit data availability |
| Cryptographic Support (FCS) | FCS_CKM.1 Cryptographic key generation |
| | FCS_CKM.4 Cryptographic key destruction |
| | FCS_COP.1Cryptographic operation |

| Security Function | Security Functional Components |
|---|---|
| User Data Protection (FDP) | FDP_IFC.1 Subset information control |
| | FDP_IFF.1 Simple security attributes |
| | FDP_RIP.2 Full residual information protection |
| Identification and Authentication (FIA) | FIA_ATD.1 User attribute definition |
| | FIA_UAU.2 User authentication before any action |
| | FIA_UAU.5 Multiple authentication mechanisms |
| | FIA_UAU.7 Protected authentication feedback |
| | FIA_UID.2 User identification before any action |
| | FIA_USB.1 User-subject binding |
| Security Management (FMT) | FMT_MOF.1 Management of security functions behavior |
| | FMT_MTD.1 Management of TSF data |
| | FMT_SMF.1 Specification of management functions |
| | FMT_SMR.1 Security Roles |
| Protection of the TSF (FPT) | FPT_FLS.1 Failure with preservation of secure state |
| | FPT_STM.1 Reliable time stamp |
| | FPT_TST.1(1) TSF Self Test |
| | FPT_TST.1(2) TSF Self Test |
| Resource Utilization (FRU) | FRU_FLT.1(1) Fault Tolerance |
| | FRU_FLT.1(2) Fault Tolerance |
| | FRU_PRS.1 Limited priority of service |
| | FRU_RSA.1 Maximum quotas |
| TOE Access (FTA) | FTA_SSL.3 TSF-initiated termination |
| | FTA_SSL.4 User-initiated termination |
| | FTA_TSE.1 TOE session establishment |
| | FTA_TAB.1 Default TOE access banners |
| Trusted Path/Channels (FTP) | FTP_TRP.1 Trusted path |

**Table 9-2: Security Functional Components for the TOE**

### 9.2.1 Security Audit

This section maps directly to the information found in Section 9.1.1. This security classification addresses the following requirements: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_STG_EXT.1, and FAU_STG.2.

FAU_ARP.1 and FAU_SAA.1 are addressed by showing the alerts that are sent via SNMP traps and by listing the events that cause the alerts to occur. FAU_GEN.1 and FAU_GEN.2 are demonstrated by showing which actions are audited (all user actions) and providing all the data that is collected in the audit logs. FAU_SAR.1 is addressed by discussing the audit logs, and showing what makes up a log, and identifying the users that are able to view the audit logs. FAU_STG.2 and FAU_STG_EXT.1 are satisfied by discussing how logs are stored and forwarded to external syslog collectors and by stating that only authorized users can delete the logs.

### 9.2.2 Cryptographic Support

This section maps directly to the information found in Section 9.1.2. This security classification addresses the following requirements: FCS_CKM.1, FCS_CKM.4, and FCS_COP.1.

FCS_CKM.1 and FCS_CKM.4 are satisfied by discussing that the TOE creates and destroys cryptographic keys. FCS_COP.1 is addressed through the discussion of the TOE utilizing SSHv2 with 256-bit AES keys.

### 9.2.3 User Data Protection

This section maps directly to the information found in Section 9.1.3. This security classification addresses the following requirements: FDP_IFC.1, FDP_IFF.1, and FDP_RIP.2

FDP_IFC.1 is addressed by discussing the enforcement of the flow control of ingress and egress traffic frames. FDP_IFF.1 is satisfied by listing the attributes used to enforce the frame forwardin and by discussing the TOE's ACL policy. FDP_RIP.2 is addressed by discussing the protection of the information of a resource on the TOE.

### 9.2.4 Identification and Authentication

This section maps directly to the information found in Section 9.1.4. This security classification addresses the following requirements: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2, and FIA_USB.1.

FIA_ATD.1 is satisfied through the discussion of attributes that are associated with each user role. FIA_UAU.2 is covered through ensuring the TOE will not allow any user to perform actions on the TOE before they are authenticated. FIA_UAU.5 is addressed by discussing the authentication methods for the TOE. Local Authentication, TACACS+, and RADIUS are all supported authentication mechanisms, in which the mechanisms also establish the claimed identity of each user. FIA_UAU.7 is addressed by discussing the message displayed to the user upon a failed logon attempt shows only that the login was unsuccessful. FIA_UID.2 is addressed by discussing how all users must be identified before being allowed to perform any action on the TOE. FIA_USB.1 is satisfied by discussing the security attributes that are associated with each user and are revoked when a user is deleted.

### 9.2.5 Security Management

This section maps directly to the information found in Section 9.1.5. This security classification addresses the following requirements: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

FMT_MOF.1 is addressed by discussing the configuration of the TOE can be affected by any user with an Admin or Super role. FMT_MTD.1 is satisfied through the list of user roles and the respective operational privileges associated with each role. FMT_SMF.1 is addressed by discussing the management functions for each role. FMT_SMR.1 is

satisfied by listing the three roles supported by the TOE. Users can be assigned to be a Super user, Admin user (on 7.2 appliances), and Limited user.

### 9.2.6 Protection of the TSF

This section maps directly to the information found in Section 9.1.6. This security classification addresses the following requirements: FPT_FLS.1, FPT_STM.1, FPT_TST.1(1) and FPT_TST.1(2).

FPT_FLS.1 is addressed by discussing the preservation of the TOE when the TOE itself or its port link(s) fail. FPT_STM.1 is addressed by discussing how the TOE has an internal clock that can be used for time stamps and that the TOE can also be configured to use an NTP server for accurate time stamps. FPT_TST.1(1) and FPT_TST.1(2) are addressed by the discussion detailing the POSTs and self tests that are run on the TOE.

### 9.2.7 Resource Utilization

This section maps directly to the information found in Section 9.1.7. This security classification addresses the following requirements: FRU_FLT.1(1), FRU_FLT.1(2), FRU_PRS.1, and FRU_RSA.1.

FRU_FLT.1(1) and FRU_FLT.1(2) are satisfied by showing how the TOE maintains throughput of the data frames any component or port in the TOE fails. FRU_PRS.1 and FRU_RSA.1 are addressed by the discussion pertaining to the allocation of bandwidth for frames traveling through the TOE.

### 9.2.8 TOE Access

This section maps directly to the information found in Section 9.1.8. This security classification addresses the following requirements: FTA_SSL.3, FTA_SSL.4, FTA_TSE.1, and FTA_TAB.1.

FTA_SSL.3 is addressed by discussing the length of time a user session is allowed to be inactive before the user is logged out of the TOE. FTA_SSL.4 is addressed by discussing how the users can log out themselves to terminate their session. FTA_TSE.1 is satisfied through the discussion of the maximum number of concurrent sessions allowed by the TOE. FTA_TAB.1 is satisfied by the discussion of banners both default and by the user.

### 9.2.9 Trusted Path/Channels

This section maps directly to the information found in Section 9.1.9. This security classification addresses the following requirement: FTP_TRP.1.

FTP_TRP.1 is addressed by discussing how users remotely connect to the TOE through encrypted channels.

# 10 Security Problem Definition Rationale

## 10.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

| Assumption | Objective | Rationale |
|---|---|---|
| A.ADMIN<br>One or more users authorized by the Operational Environment will be assigned to install, configure and manage the TOE and the security of the information it contains. | OE.ADMIN<br>One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains. | OE.ADMIN maps to A. ADMIN in order to ensure that only the users authorized by the TOE will install and configure the TOE to bring it into the evaluated configuration. During operation only the users authorized by the TOE will be able to manage the TOE in a manner that maintains its ADMIN objectives. |
| A.CPE<br>Service Delivery Switches will only be deployed to connect to Customer Premise Equipment. | OE.CPE<br>Service Delivery Switches must only be deployed to connect to Customer Premise Equipment. | OE.CPE directly maps to A.CPE to ensure that only Customer Premise Equipment is used to connect to the TOE. |
| A.LOCATE<br>The TOE will be located within controlled access facilities that will prevent unauthorized physical access. | OE.LOCATE<br>The TOE will be located within controlled access facilities that will prevent unauthorized physical access. | OE.LOCATE maps to A.LOCATE in order to ensure that physical security is provided in the environment where the TOE operates. |
| A.NOEVIL<br>Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. | OE.NOEVIL<br>All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. | OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided. |
| A.PASSWORD<br>Users select passwords according to the strong password policy that has been configured by an administrative user and will protect their own authentication data. | OE.PASSWORD<br>All users of the TOE will select appropriately strong passwords and will protect their own authentication data. | OE.PASSWORD maps to A.PASSWORD in order to ensure that user authentication data is sufficiently secure and therefore that the authentication mechanism itself is more secure. |
| A.PROTECT<br>The operational environment must protect the channel to the configured syslog collectors from interruption using logical methods, such as encryption, or physical methods such as disconnecting the TOE from internet and storing it in the same secure location. | OE. PROTECT<br>All channels to the configured syslog collectors will be protected from interruption using logical (encryption) or physical (disconnecting from the internet) methods. | OE.PROTECT maps to A.PROTECT in order to ensure that the TOE channels to external servers are protected with secure methods. |

**Table 10-1: Assumption to Objective Mapping**

| Threat | Objective | Rationale |
|---|---|---|
| T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions. | O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE. | O.ACCESS (FAU_ARP.1, FAU_SAA.1, FCS_COP.1, FDP_IFC.1, FDP_IFF.1, FIA_ATD.1, FIA_USB.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1) helps mitigate this threat by providing authorized users the ability to determine the access levels of authenticated users through the assignment and enforcement of roles. |
| | O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE. | O.MANAGE (FMT_MOF.1, FMT_MTD.1, FMT_SMF.1) helps to mitigate this threat by providing the authorized users of the TOE with the capability to specify access rights to protected TOE resources to authenticated TOE users. |
| | OE.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access. | OE.LOCATE helps to mitigate this threat by ensuring that local access to the TOE is protected against unauthorized physical access. |
| T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms. | O.DISPLAY_BANNNER The TOE will display an advisory warning regarding use of the TOE. | O.DISPLAY_BANNER (FTA_TAB.1) helps mitigate this threat by providing message advising the administrator of the proper use of the TOE. |
| | O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE. | O.MANAGE (FMT_MOF.1, FMT_MTD.1, FMT_SMF.1) helps mitigate this threat by providing authorized users the ability to configure the TOE within a secure state or return the TOE to a secure state. |
| | OE.ADMIN<br>One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains. | OE.ADMIN helps mitigate this threat by ensuring that at least one administrator will be properly trained in the installation and management of the TOE to place it into the proper evaluated configuration. |
| | OE.NOEVIL<br>All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. | OE.NOEVIL helps mitigate this threat by ensuring that staff authorized to install and/or operate the TOE are sufficiently vetted by the organization deploying the TOE. |

| Threat | Objective | Rationale |
|---|---|---|
| T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause the records or information to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action. | O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE | O.ACCESS (FIA_USB.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1) helps mitigate this threat by providing authorized users the ability to determine the access levels of authenticated users through the assignment and enforcement of roles, such that only users explicitly authorized to perform an action can perform one. |
| | O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded. | O.ALERT (FAU_ARP.1, FAU_SAA.1) helps mitigate this threat by providing functionality to generate and send alerts based upon definable criteria such that if an alert condition is triggered, an authorized user will be notified within a suitable timeframe. |
| | O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE. | O.AUDIT (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG_EXT.1, FAU_STG.2) helps mitigate this threat by assuring that all security-relevant actions are audited such that all misuse of the TOE can be tracked to the malicious user. |
| | O.SYSTIME The TOE will provide reliable system time. | O.SYSTIME (FPT_STM.1) helps mitigate this threat by assuring that all audit logs will have appropriate timestamps applied to them to pinpoint the exact time a malicious action occurred. |
| | OE. PROTECT<br>All channels to the configured syslog collectors will be protected from interruption using logical (encryption) or physical (disconnecting from the internet) methods. | OE.PROTECT helps mitigate this threat by ensuring that the audit data sent to external syslog collectors is appropriately protected by the environment in which the TOE is deployed. |
| T.DATA_COMPROMISE A malicious user or process may attempt to gain unauthorized access and/or obtain resources controlled by the TOE that have been allocated during a TOE operational session. | O.DEALLOCATION The TOE will provide measures to perform deallocation of memory from a TOE object when a session has been ended. | O.DEALLOCATION (FDP_RIP.2) helps mitigate this threat by ensuring that the TOE will deallocate memory from a user session to ensure no data is left vulnerable to an attack. |

| Threat | Objective | Rationale |
|---|---|---|
| T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. | O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data. | O.EAVESDROPPING (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_TRP.1) helps mitigate this threat by ensuring that all external communication to and from the TOE is encrypted with cryptographic keys of appropriate strength. |
| T.NETWORK_FLOW A malicious user may attempt to subvert the TOE or defeat the operation of its security mechanisms to cause a disruption in the flow of data on the production network. | O.MAP The TOE will provide mechanisms to set and control the association of physical data identifiers and logical data identifiers with the TOE services | O.MAP (FDP_IFC.1, FDP_IFF.1) helps mitigate this threat by ensuring that all physical and logical data identifiers are controlled through the TOE and TOE services. |
| | O.NETWORK_FLOW_PROTECTION The TOE will preserve the information flow of the production network data through the TOE in the presence of adversarial activity when a component of the TOE fails. | O.NETWORK_FLOW_PROTECTION (FPT_FLS.1, FPT_TST.1(1), FPT_TST.1(2), FRU_FLT.1(1), FRU_FLT.1(2), FRU_PRS.1, FRU_RSA.1) helps mitigate this threat by ensuring that the TOE has means to protect itself and its core functionality in the event of the system being unexpectedly brought down as well as perform self-testing to ensure proper functionality. |
| | OE.CPE Service Delivery Switches must only be deployed to connect to Customer Premise Equipment. | OE.CPE requires Service Delivery Switches to be connected and authenticated to Customer Premise Equipment, giving reasonable assurance that the connected devices are trusted. |
| | OE.LOCATE<br>The TOE will be located within controlled access facilities that will prevent unauthorized physical access. | OE.LOCATE helps to mitigate this threat by ensuring that local access to the TOE is protected from unauthorized personnel such that the TOE's hardware is not accessible. |

| Threat | Objective | Rationale |
|---|---|---|
| T.MASK Users whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures. | O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE. | O.AUTH (FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2, FIA_USB.1) helps mitigate this threat by requiring users to have appropriate user accounts on the TOE with appropriate secrets such that a malicious user could not easily gain access to another user's account. |
| | O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate. | O.ROBUST_TOE_ACCESS (FTA_SSL.3, FTA_SSL.4, FTA_TSE.1) helps mitigate this threat by providing mechanisms by ensuring that inactive sessions are appropriately closed, denying session establishments based on criteria, and providing a secure logout functionality for legitimate users. |
| | OE.NOEVIL All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. | OE.NOEVIL helps to mitigate this threat by ensuring that those individuals who are given authorization to access the TOE have been screened or interviewed during the hiring process to ensure they do not have any malicious intent. |
| | OE.PASSWORD All users of the TOE will select appropriately strong passwords and will protect their own authentication data. | OE.PASSWORD helps to mitigate this threat by ensuring that users select strong passwords preventing a malicious user from guessing or brute forcing the password information. |
| T.STEALTH A malicious user or process could perform suspicious activities against the TOE or objects in the Operational Environment monitored by the TOE without a TOE user authorized by the TOE or Operational Environment becoming aware of this. | O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded. | O.ALERT (FAU_ARP.1, FAU_SAA.1) helps to mitigate this threat by providing users with the ability of receiving alert notifications from the TOE when events are considered to be a security violation based upon a defined policy. |

| Threat | Objective | Rationale |
|---|---|---|
| | O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE. | O.AUDIT (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG_EXT.1, FAU_STG.2) helps mitigate this threat by providing audit records which allow users to determine what users attempt to perform and when they attempt to perform it. |
| | O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE. | O.AUTH (FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2, FIA_USB.1) helps mitigate this threat by ensuring that all users that try and access the TOE become identified and authenticated before any access is granted. |
| | O.MAP The TOE will provide mechanisms to set and control the association of physical data identifiers and logical data identifiers with the TOE services. | O.MAP (FDP_IFC.1, FDP_IFF.1) helps mitigate this threat by creating and enforcing flow control policies to control user flow. |
| | OE.NOEVIL All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation. | OE.NOEVIL helps to mitigate this threat by ensuring that those individuals who are given authorization to access the TOE have been screened or interviewed during the hiring process to ensure they do not have any malicious intent. |

**Table 10-2: Threat to Objective Mapping**

## 10.2 Operational Security Policy Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated organizational security policy.

| OSP | Objective | Rationale |
|---|---|---|
| P.ACCESS_BANNER<br>The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. | O.DISPLAY_BANNER<br>The TOE will display an advisory warning regarding use of the TOE. | O.DISPLAY_BANNER (FTA_TAB.1) satisfies this policy by ensuring that the TOE displays a Security Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE. |

**Table 10-3: Operational Security Policy to Objective Mapping**

### 10.3 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE objectives.

| Objective | Security Functional Components | Rationale |
|---|---|---|
| O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE. | FCS_COP.1 Cryptographic Operation | FCS_COP.1 describes the encryption that is in place to ensure access is secure. |
| | FDP_IFC.1 Subset Information Flow Control | FDP_IFC.1 describes the flow control policy that is enforced on user access to the TOE. |
| | FDP_IFF.1 Simple Security Attributes | FDP_IFF.1 details the security attributes and rules that are taken into account when enforcing the flow control policy. |
| | FIA_ATD.1 User attribute definition | FIA_ATD.1 shows all of the user attributes that are utilized to authorize users, including user role. |
| | FIA_USB.1 User-subject binding | FIA_USB.1 shows how users and their roles are associated in a session. |
| | FMT_MOF.1 Management of security functions behavior | FMT_MOF.1 defines the functions that can be performed by specific roles within the TOE. |
| | FMT_MTD.1 Management of TSF data | FMT_MTD.1 defines the specific actions that specific roles can perform on specific data sets within the TOE. |
| | FMT_SMF.1 Specification of Management Functions | FMT_SMF.1 defines the functions that can be performed by specific types of users of the TOE. |
| | FMT_SMR.1 Security roles | FMT_SMR.1 defines that there are roles in the system and that users are associated with their role for making authorization decisions. |
| O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded. | FAU_ARP.1 Security alarms | FAU_ARP.1 requires the TOE to provide mechanisms to alert authorized users in the event of a security violation. |
| | FAU_SAA.1 Potential violation analysis | FAU_SAA.1 requires the TOE to provide mechanisms to determine if a security violation has taken place. With both this and FAU_ARP.1, the TOE will detect violations and alert authorized users appropriately. |
| O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE. | FAU_GEN.1 Audit data generation | FAU_GEN.1 defines the behavior of the TSF which causes security relevant events to be generated and enumerates the data which is contained within these events. |
| | FAU_GEN.2 User identity association | FAU_GEN.2 confirms that all relevant auditable events include subject identity for the purposes of accountability. |
| | FAU_SAR.1 Audit review | FAU_SAR.1 provides the ability for all authorized users to read audit data using the UIs. |

| Objective | Security Functional Components | Rationale |
|---|---|---|
| | FAU_STG_EXT.1 Protected Audit Trail Storage | FAU_STG_EXT.1 confirms that the TOE transfers generated audit data through a trusted channel to an external IT entity. |
| | FAU_STG.2 Guarantees of audit data availability | FAU_STG.2 states that only authorized users can use the TOE functionality that exists to modify or delete audit records and that the oldest logs will be deleted once storage is exhausted. |
| O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE. | FIA_ATD.1 User attribute definition | FIA_ATD.1 defines the security-relevant attributes of all users. This includes attributes related to authentication. |
| | FIA_UAU.2 User authentication before any action | FIA_UAU.2 requires users to authenticate to the TOE before any TSF-mediated actions are allowed. |
| | FIA_UAU.5 Multiple authentication mechanisms | FIA_UAU.5 defines the various authentication mechanisms in the TOE: local authentication, RADIUS, and TACACS+. |
| | FIA_UAU.7 Protected Authentication Feedback | FIA_UAU.7 states that it provides simple password failed messages to users if authentication is unsuccessful. |
| | FIA_UID.2 User identification before any action | FIA_UID.2 requires users to identify themselves to the TOE before any TSF-mediated actions are allowed. |
| | FIA_USB.1 User-subject binding | FIA_USB.1 defines the mapping between users and roles and the creation of a session. |
| O.DEALLOCATION The TOE will provide measures to perform deallocation of memory from a TOE object when a session has been ended. | FDP_RIP.2 Full Residual Information Protection | FDP_RIP.2 ensures that the data in memory that was allocated to a user session goes through deallocation once the session has ended. |
| O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE. | FTA_TAB.1 Default TOE access banners | FTA_TAB.1 requires the TOE to provide a warning banner to users prior to authentication. |
| O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data. | FCS_CKM.1 Cryptographic key generation | FCS_CKM.1 requires the TOE to generate proper cryptographic keys for use in encrypting sensitive data. |
| | FCS_CKM.4 Cryptographic key destruction | FCS_CKM.4 requires the TOE to destroy cryptographic keys used in encrypting sensitive data. Keys are destroyed when new keys are generated. |
| | FCS_COP.1 Cryptographic operation | FCS_COP.1 requires the TOE to utilize the generated cryptographic |

| Objective | Security Functional Components | Rationale |
|---|---|---|
| | | keys in protecting all data transferred to and from users, other TOE components, and external IT products. |
| | FTP_TRP.1 Trusted path | FTP_TRP.1 requires the TOE to make all security-relevant data sent to and from users protected against modification. This is done by creating a trusted path with the encryption mechanisms described in FCS_COP.1. |
| O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE. | FMT_MOF.1 Management of security functions behavior | FMT_MOF.1 defines the functions that can be performed by specific roles within the TOE. |
| | FMT_MTD.1 Management of TSF data | FMT_MTD.1 defines the specific actions that specific roles can perform on specific data sets within the TOE. |
| | FMT_SMF.1 Specification of Management Functions | FMT_SMF.1 defines the functions that can be performed by specific types of users of the TOE. |
| O.MAP The TOE will provide mechanisms to set and control the association of physical data identifiers and logical data identifiers with the TOE services. | FDP_IFC.1 Subset information control | FDP_IFC.1 details the subjects and objects defined and controlled within the flow control policy. |
| | FDP_IFF.1 Simple security attributes | FDP_IFF.1 details the security attributes and rules that are taken into account when enforcing the flow control policy. |
| O.NETWORK_FLOW_PROTECTION The TOE will preserve the information flow of the production network data through the TOE in the presence of adversarial activity when a component of the TOE fails. | FPT_FLS.1 Failure with preservation of secure state | FPT_FLS.1 requires the TOE to remain in a secure state when the TOE fails. |
| | FRU_FLT.1(1) Fault tolerance | FRU_FLT.1(1) requires that the TOE's management and control plane remains operational in the occurance of a failure with a single management Control Card within a chassis-based TOE. |
| | FRU_FLT.1(2) Fault tolerance | FRU_FLT.1(2) requires that the TOE's data flow functionality remains operational in the occurrence of a breakage of a server link within a system with redundant physical links. |
| | FRU_PRS.1 Limited Priority of Service | FRU_PRS.1 describes that the TOE sets a priority to each subject in the TSF to ensure bandwidth access is mediated. |
| | FRU_RSA.1 Maximum Quotas | FRU_RSA.1 describes how the TSF will enforce a maximum quota on usage for the bandwidth that users can use simultaneously. |
| | FPT_TST.1(1) TSF Self-Test | FPT_TST.1(1) describes how the |

| Objective | Security Functional Components | Rationale |
|---|---|---|
| | | TOE runs a suite of self tests during startup, after failure, or when manually selected to demonstrate correct operation of the TSF. |
| | FPT_TST.1(2) TSF Self-Test | FPT_TST.1(2) describes how the TOE runs a suite of self tests during startup, after failure, or when manually selected to demonstrate correct operation of the TSF. |
| O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate. | FTA_SSL.3 TSF-initiated termination | FTA_SSL.3 helps the TOE offer granular controls to provide access to TOE resources by providing functionality to automatically terminate a user's session if they are idle or away from their terminal. |
| | FTA_SSL.4 User-initiated termination | FTA_SSL.4 helps the TOE offer protection of TOE access by presenting users the ability to securely log out of the UI. |
| | FTA_TSE.1 TOE Session Establishment | FTA_TSE.1 describes the ability of the TSF to deny session establishment based on criteria. |
| O.SYSTIME The TOE will provide reliable system time. | FPT_STM.1 Reliable time stamp | FPT_STM.1 requires the TOE to maintain accurate system time to provide for time stamping purposes. |

**Table 10-4: Security Functional Requirements Rationale**

## 10.4 EAL2 Justification

The threats that were chosen are consistent with an attacker of basic attack potential, therefore EAL2 was chosen for this ST.

## 10.5 Requirement Dependency Rationale

The table below lists each requirement from claimed Security Functional Requirements with a dependency and indicates whether the dependent requirement is included. If a dependency has not been met, a short rationale is provided to show why the dependency is not included.

| Functional Component | Dependency | Included |
|---|---|---|
| FAU_ARP.1 | FAU_SAA.1 | YES |
| FAU_GEN.1 | FPT_STM.1 | YES |
| FAU_GEN.2 | FAU_GEN.1, FIA_UID.1 | YES |
| FAU_SAA.1 | FAU_GEN.1 | YES |
| FAU_SAR.1 | FAU_GEN.1 | YES |
| FAU_STG.2 | FAU_GEN.1, FPT_ITC.1 | YES (FAU_GEN.1) |
| FCS_CKM.1 | FCS_CKM.2 or FCS_COP.1 | YES (FCS_COP.1) |
| FCS_CKM.4 | FDP_ITC.2 or FCS_CKM.1 | YES (FCS_CKM.1) |
| FCS_COP.1 | FDP_ITC.1 , FDP_ITC.2 or FCS_CKM.1 | YES (FCS_CKM.1) |
| | FCS_CKM.4 | YES |
| FDP_IFC.1 | FDP_IFF.1 | YES |

| | | |
|---|---|---|
| FDP_IFF.1 | FDP_IFC.1 or FMT_MSA.3 | YES (FDP_IFC.1) |
| FIA_UAU.2 | FIA_UID.1 | YES (Hierarchy: FIA_UID.2) |
| FIA_UAU.7 | FIA_UAU.1 | YES (Hierarchy: FIA_UAU.2) |
| FIA_USB.1 | FIA_ATD.1 | YES |
| FMT_MOF.1 | FMT_SMR.1, FMT_SMF.1 | YES |
| FMT_MTD.1 | FMT_SMR.1, FMT_SMF.1 | YES |
| FMT_SMR.1 | FIA_UID.1 | YES (Hierarchy: FIA_UID.2) |
| FRU_FLT.1(1) | FPT_FLS.1 | YES |
| FRU_FLT.1(2) | FPT_FLS.1 | YES |

**Table 10-5: Requirement Dependencies**

## 10.6 Assurance Measures

The SARs for this evaluation have been chosen because they are consistent with the package claim of EAL2.

The following table identifies the SARs for this ST. Note that "Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2" also represents the TOE in this instance. During the course of the evaluation the same product was re-branded by the vendor as "Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2". Therefore, any documentation which references ActivEdge is considered to accurately represent the TOE.

| Component | Document(s) | Rationale |
|---|---|---|
| ADV_ARC.1<br>Security Architecture Description | TOE Design Specification document for Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2 | This document describes the security architecture of the TOE. |
| ADV_FSP.2<br>Security-enforcing functional specification | Functional Specification Document for Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2 | This document describes the functional specification of the TOE with complete summary. |
| ADV_TDS.1<br>Basic Design | TOE Design Specification document for Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2 | This document describes the architectural design of the TOE. |

| Component | Document(s) | Rationale |
|---|---|---|
| AGD_OPE.1<br>Operational User Guidance | • SAOS Software Configuration Guide Release 6.10.2<br>• SAOS Software Configuration Guide 7.2<br>• SAOS CLI Reference Manual Release 6.10.2<br>• SAOS CLI Command Reference 7.2<br>• 5150 Service Aggregation Switch Hardware Installation Manual<br>• 3930 Service Delivery Switch Hardware Installation Manual<br>• SAOS Release Notes Release 6.10.2.140<br>• 5410 and 5305 Service Aggregation Switches SAOS Software Release Notes: SAOS 7.2.0.585 | These documents describe the operational user guidance for the TOE. |
| AGD_PRE.1<br>Preparative Procedures | • SAOS Software Configuration Guide Release 6.10.2<br>• SAOS Software Configuration Guide 7.2<br>• SAOS CLI Reference Manual Release 6.10.2<br>• SAOS CLI Command Reference 7.2<br>• 5150 Service Aggregation Switch Hardware Installation Manual<br>• 3930 Service Delivery Switch Hardware Installation Manual<br>• SAOS Release Notes Release 6.10.2.140<br>• 5410 and 5305 Service Aggregation Switches SAOS Software Release Notes: SAOS 7.2.0.585 | These documents describe the preparative procedures that need to be done prior to installing the TOE. |
| ALC_CMC.2<br>Use of a CM system | • Ciena_CESD_SCM<br>• CO2-CMG-01<br>• CO2-CMG-05 | These documents describe the authorization controls for the TOE. |
| ALC_CMS.2<br>Parts of the TOE CM coverage | • 6x-main.txt<br>• 7x-main.txt<br>• Docs.txt<br>• Agile Snapshots folder | These documents describe the CM scope of the TOE. |
| ALC_DEL.1<br>Delivery Procedures | CO2-MAT-02 | This document describes product delivery for the TOE and a description of all procedures used to ensure objectives are not compromised in the delivery process. |

| Component | Document(s) | Rationale |
|---|---|---|
| ASE_CCL.1<br>Conformance Claims | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document describes the CC conformance claims made by the TOE. |
| ASE_ECD.1<br>Extended Components Definition | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document provides a definition for all extended components in the TOE. |
| ASE_INT.1<br>Security Target Introduction | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document describes the Introduction of the Security Target. |
| ASE_OBJ.2<br>Security Objectives | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document describes all of the security objectives for the TOE. |
| ASE_REQ.2<br>Derived Security Requirements | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document describes all of the security requirements for the TOE. |
| ASE_SPD.1<br>Security Problem Definition | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | This document describes the security problem definition of the Security Target. |
| ASE_TSS.1<br>TOE Summary Specification | Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.10.2 and 7.2 | These documents describe the TSS section of the Security Target. |
| ATE_COV.1<br>Evidence of Coverage | • Functional Specification Document for Ciena ActivEdge Service Delivery/Aggregation Switch with SAOS versions 6.10.2 and 7.2<br>• Test Plans folder | These documents provide an analysis of coverage for the TOE. |
| ATE_FUN.1<br>Functional Testing | Test Plans folder | These documents describe the functional tests for the TOE. |
| ATE_IND.2<br>Independent Testing - sample | Ciena Corporation ActivEdge Service Delivery/Aggregation Switch with SAOS Versions 6.10.2 and 7.2 Evaluation Team Test Report | This document describes the independent testing for the TOE. |
| AVA_VAN.2<br>Vulnerability Analysis | Ciena Corporation ActivEdge Service Delivery/Aggregation Switch with SAOS Versions 6.10.2 and 7.2 Vulnerability Analysis | This document describes the vulnerability analysis of the TOE. |

**Table 10-6: Assurance Requirements Evidence**