Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3

Security Target
Revision 11
October 19, 2005

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.2 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 2.1.4 of Part 2 of the CC [CC2] are *refinement, selection, assignment* and *iteration.*

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

All operations described above are used in this Security Target. *Italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

References

[CC1] Common Criteria Part 1: Introduction and General Model, Version 2.2, January 2004, Revision 256, CCIMB-2004-01-001.

[CC2] Common Criteria Part 2: Security Functional Requirements, Version 2.2, January 2004, Revision 256, CCIMB-2004-01-002.

[CC3] Common Criteria Part 3: Security Assurance Requirements, Version 2.2, January 2004, Revision 256, CCIMB-2004-01-003.

Document Organization

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3 [CC2, CC3], respectively that must be satisfied by the TOE.

Section 6 identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Section 7 makes any protection profile claims applicable to the TOE.

Section 8 provides a rationale to explicitly demonstrate that the security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Section 8 also provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the security target requirements.

Appendix A documents an acronym list and glossary to define frequently used acronyms applicable to the TOE.

1 Introduction

This introductory section presents *security target (ST)* identification information and an overview of the ST. A statement of Common Criteria conformance is also provided.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE).

ST Title:	Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Security Target
ST Revision:	11
ST Publication Date:	October 19, 2005
TOE Identification:	Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform operating ONS 15454 software release 4.1.3 on the following timing, communications, and control cards: • 15454-TCC2 (SONET) • 15454E-TCC2 (SDH)
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 (Revision 256) with the following NIAP Interpretation: I-0432.
ST Evaluation:	National Information Assurance Partnership
Assurance Level:	Evaluation Assurance Level 2
Author(s):	Cisco Systems, Inc. & Decisive Analytics Corp.
Keywords:	ONS 15454, MSPP, TCC2

1.2 Security Target Overview

This Security Target defines the security functionality provided by the Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform (MSPP) operating ONS 15454 software release 4.1.3 (hereafter referred to as the TOE). The TOE is focused on metropolitan and regional optical transport networks by providing high-density aggregation of voice, video, and data, as well as storage protocols over a SONET/SDH network. The TOE can be configured to provide the functions of multiple network elements while supporting a variety of electrical, Ethernet, and optical-based interfaces.

The TOE software resides on the Timing, Communications, and Control Card, Version 2.0 (TCC2) for both SONET (15454-TCC2) and SDH (15454E-TCC2) optical-based networks. The TCC2 is the main processing card for the ONS 15454 and provides system initialization, provisioning, alarm reporting, maintenance, security functions and diagnostics. Through the TCC2, the TOE implements the functions relevant to the secure operation and management of a typical ONS 15454 system deployment.

1.3 Common Criteria Conformance

The ST claims conformance to CC Version 2.2 Part 2 [CC2] extended, with the following NIAP Interpretation applied: I-0432.

The TOE is conformant with Part 3 of the CC, Version 2.2 [CC3], and specifically claims conformance to the Evaluation Assurance Level 2 (EAL2).

2 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Overview of the Product (TOE)

Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform

The primary function of the TOE is to provide the underlying infrastructure for metropolitan/regional optical transport networks. The TOE supports the provisioning of multiple network platforms including Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) traffic as well as emerging services in these networks – Dense Wavelength Division Multiplexing (DWDM), Multi Protocol Line Switching (MPLS) and Storage Area Networks (SANs). Traditional transport services such as Ethernet, IP, and Time Division Multiplexing (TDM) are also supported by the TOE.

The ONS 15454 provides a single platform solution to aggregate access network traffic (e.g. routers, Data Link Connections (DLCs), Digital Subscriber Line Access Multiplexers (DSLAMs), Integrated Access Devices (IADs), cable modems, edge switches, etc.), multiplex that traffic to traverse metropolitan/regional optical networks and provide an interface to the Internet Point of Presence (PoP) or optical core. The multiservice interfaces and integrated optical networking for all rates and topologies provides for cost-effective economics for Optical Carriers (OCs). The TOE allows system operators to terminate multiple rings or linear systems on a single chassis; mixing and matching the service interfaces that enable a unified data, voice, and video network. This network architecture is shown in Figure 1.

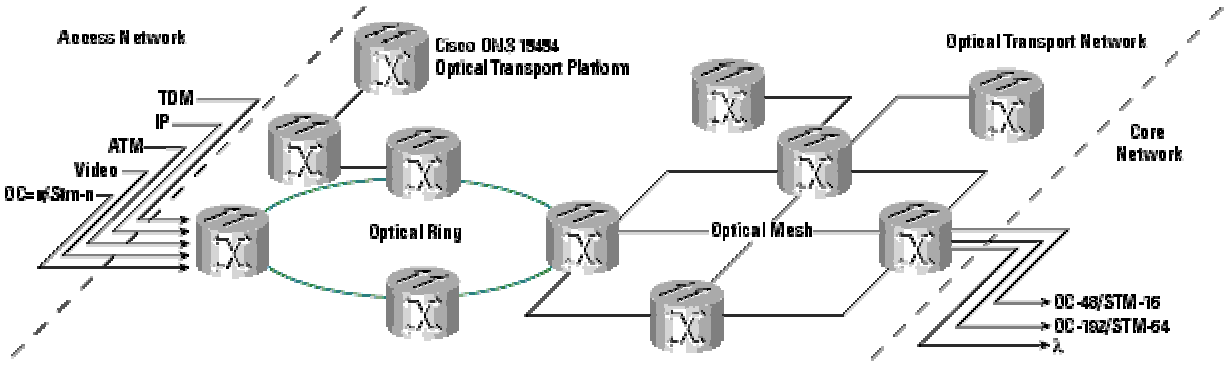

Figure 1 - Multiservice Optical Network Architecture

ONS 15454 Shelf Assembly

The ONS 15454 shelf assembly (SA) is shown in Figure 2. The SA contains 17 plug-in card slots, a backplane interface and a fan tray. The fan tray incorporates a front panel with a Liquid Crystal Display (LCD) and the alarm indicators. When installed in an equipment rack, the SA is typically connected to a fuse and alarm panel to provide centralized alarm connection points and distributed

power for the ONS 15454. The front door of the ONS 15454 allows access to the SA, fan tray, and cable management area[1]. The backplane provides access to alarm contacts, external interface contacts, power terminals, and various network connectors.

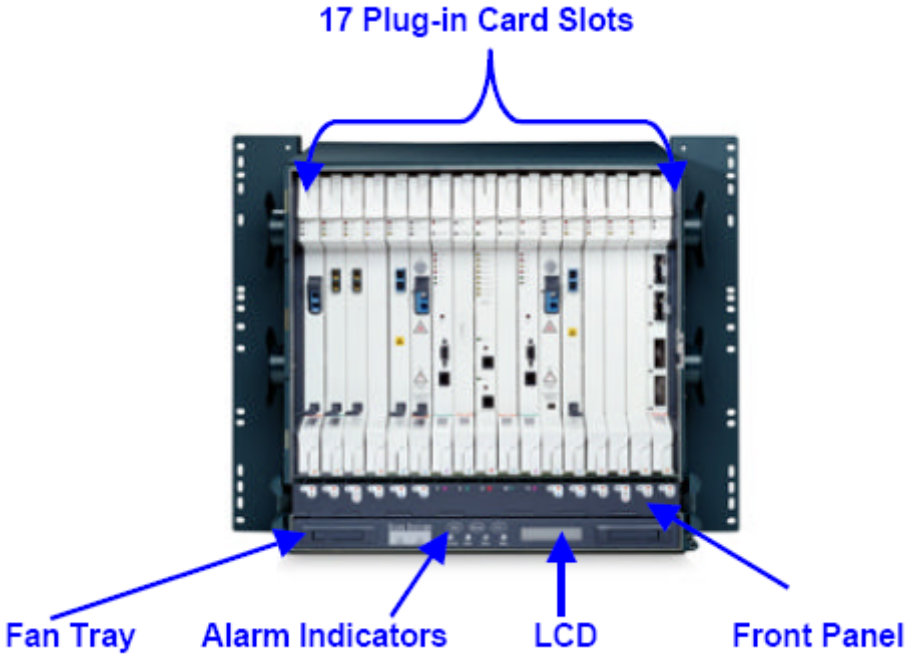

Figure 2 – ONS 15454 SONET Shelf Assembly

The TOE security functions are provided by the timing, communications, and control cards residing in slots 7 and 11 of the SA (as depicted in Figure 3). Cards residing in the remaining slots do not contribute nor interfere with the security functionality of the TOE. The SA backplane (where the cards interface with the transport networks and the other cards) does not contribute directly to the TSF, however, some of its interfaces are used to support the TSF. Please refer to section 2.2 for additional information concerning the security relevancy of the SA backplane interfaces.

[1] The ONS 15454 SDH has an additional Electrical Facility Connection Assembly (EFCA) located at the top of the shelf. The EFCA provides the administrator with front access to the card connectors.

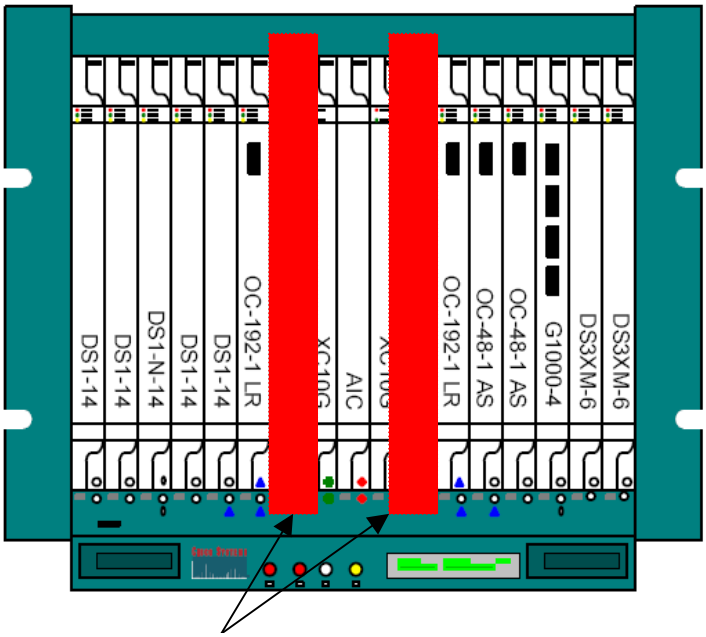

Figure 3 – ONS 15454 Shelf Assembly with TCC2 cards installed

Timing, Communications, and Control Card Version 2.0

The TCC2 is the main processing card for the ONS 15454 providing system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET/SDH Data Communications Channel (DCC) termination, and system fault detection. The TOE software resides on the TCC2 for both SONET and SDH network platforms. In addition, all of the TOE security features (refer to section 2.3) are implemented on the TCC2.

Non-volatile database storage for communication, provisioning, and system control is provided on the TCC2 to allow for database recovery should a system power failure occur. The TCC2 also originates and terminates a cell bus carried to each card slot via point-to-point links over the backplane. The cell bus supports links between any two cards in the node, which is essential for peer-to-peer communication.

The TCC2 has its own internal system clock which is used by the TOE for reliable time stamps. The system clock can be set via manual input (i.e. directly by the administrator) or be configured to synchronize with a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server. Further discussion on the physical scope of the TOE has been provided in section 2.2.

As indicated by Figure 3, the TCC2 is installed in the ONS 15454 SA in a redundant configuration. Please note that while typical ONS 15454 deployments will contain a redundant TCC2 card, this ST does not claim any security features related to the availability of the system. Furthermore, the security functionality resulting through such a redundant configuration is not part of the evaluation.

ONS 15454 Management

The ONS 15454 is managed through the TCC2 using the management applications and interfaces defined in this section. Management must be performed locally either through the Ethernet or RS-232 serial interfaces in accordance with the evaluated configuration. Please note that the serial interface is not supported by the SDH platform. The following management applications or protocols are used to manage the evaluated TOE:

- TL1 – Transaction Language 1
  TL1 provides a standard set of messages that are used for communicating between operating systems and network elements, and personnel and network elements. TL1 commands can be accessed using VT100 emulation over a telnet session. Please note that the TL1 interface implemented by the ONS 15454 can only manage a limited subset of the security functions, and is not supported by the SDH platform.

- CTC – Cisco Transport Controller
  The CTC is a web-based graphical user interface (GUI) application capable of managing all of the security functions, as well as performing the provisioning and administration functions of the TCC2.

Please note that the management interfaces and applications do not implement the TOE security functions defined by this ST. Furthermore, the scope of the TOE is limited to the CTC interface and/or the TL1 interface to manage the security functions (i.e. the application software is excluded from the scope of the TOE).

ONS 15454 Evaluated Components (High-Level)

Figure 4 illustrates the high-level logical scope of the TOE. As noted by the figure, SNMP functionality, the NTP server, and other ONS 15454 cards are not within scope of the evaluation. The following high-level components are within the logical scope of the TOE:

- The TCC2 card, as described above. The TCC2 is connected to ONS 15454 shelf assembly via the backplane interfaces (which are within scope of the evaluation). These interfaces are shown in Figure 5 and discussed in Table 1 below. The TCC2 card contains the ONS 15454 system software and the internal system clock which together implement the TOE security functions.
- The TL1 and CTC management interfaces, as described above. The CTC and TL1 applications provide the management interface to the TOE security functions (via the TCC2 serial and Ethernet ports). The applications themselves are not part of the TOE, as all security processing is performed on the TCC2 card.

Please refer to section 2.2 for an explanation of the TOE physical scope and boundary for further information.

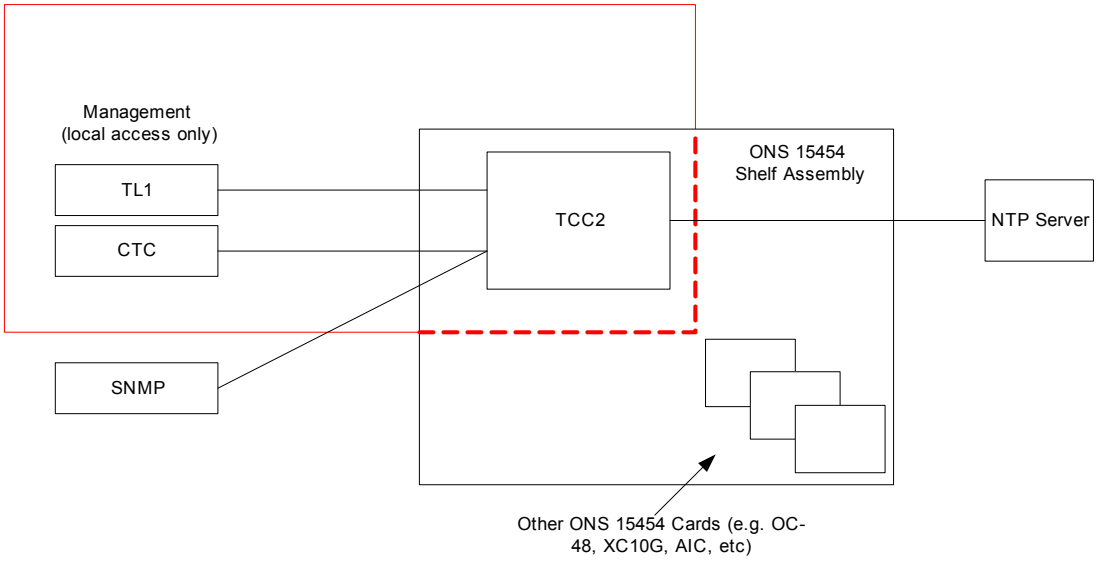

Figure 4 – Logical Scope of the TOE

2.2 Physical Scope of the TOE

The software and hardware components that comprise the TOE are defined in this section.

2.2.1 TOE Software and Hardware

In order to comply with the evaluated configuration, the following hardware and software components should be used:

Table 1 – Evaluated Configuration for the TOE

TOE Component	Part Number	Cisco Part Number, Revision
TOE Software	15454-0413-003L-1901 (SONET CD Version)	15454-R4.1.3SWCD, A0
	15454SDH-0413-003L-1901 (SDH CD Version)	15454E-R4.1.3SWCD, A0
	15454-0413-003L-1901 (SONET Pre-loaded Version)	SF15454-R4.1.3, A0
	15454SDH-0413-003L-1901 (SDH Pre-loaded Version)	SF15454E-R4.1.3, A0

TOE Component	Part Number	Cisco Part Number, Revision
	15454-0413-003L-1901 (SONET Upgrade License)	15454-LIC-R4.1.3, A0
	15454SDH-0413-003L-1901 (SDH Upgrade License)	15454E-LIC-R4.1.3, A0
TOE Hardware	15454-TCC2	ONS 15454 Timing, Communications, and Control Card, Version 2 (SONET only)
TOE Hardware	15454E-TCC2	ONS 15454 Timing, Communications, and Control Card, Version 2 (SDH only)

In addition to using the above mentioned software and hardware versions, users should ensure that the TOE is installed, configured and maintained in accordance with this document and the associated user guidance. In this context, the TOE is considered a single node with DCC connections to another TOE, which has been configured consistent with the Common Criteria evaluated configuration, and to which are applied the same physical, operational, and administrative controls. Users in the context of this ST are external subjects; comprising authorized users whose user name and password are contained in the provisioning database and are therefore authorized to access the ONS 15454 according to their assigned privilege level. Unauthorized users are those external subjects that are not contained in the provisioning database, and therefore viewed in a threat context. The document titled *Installation and Configuration for the Common Criteria EAL2 Evaluated Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform* is an addendum to the user guidance documentation and must be followed in order to comply with the evaluated configuration. This addendum must also be read first prior to becoming familiar with the remainder of the user guidance documentation.

2.3 Security Features

The high-level logical scope of the TOE has been depicted in **Figure 4** above. The security functionality of the TOE is implemented by the ONS 15454 system software and the system clock which both reside on the TCC2 card. In concert, these two components implement the security features claimed by this ST (i.e. the TSF), and are summarized in Table 2 below.

Table 2 – Summary of TOE Security Features

Feature	Description
Security Management Roles	Up to 500 users IDs can be assigned to one of four privilege levels and privileges and actions associated with those levels.

Feature	Description
Superuser Privilege and Login	The TOE provides Superuser privileges, so that only the Superuser can create, or delete, other users. The Superuser privilege provides that level user with sole responsibility for the security of the nodes. These privileges include the ability to view and monitor the list of logged in users, and the ability to log off and to change the privilege level of any user.
Security Management	Concurrent user sessions are permitted on the node, such that multiple users can log into a node using that user ID. The Superuser can provision the privilege level such that a single user ID within that privilege level can only be active in a single login occurrence on any given node.
Security Alarm Events	Security thresholds can be defined and set so that a user can only be permitted that number of invalid login attempts before that user ID is locked out. A violation of those security thresholds generates an alarm and the alarm event is recorded in the audit trail. There are also alarm events for audit trail reaching 80% capacity and audit trail 100% capacity
Audit Trail	The audit trail records user actions such as login, logout, circuit creation, and circuit deletion. It also records security events such as failed login attempts, etc. Audit trails can be off-loaded and stored for later review and analysis.
Login Control	Allows definition of the number of invalid login attempts that a user ID is allowed to make before that user ID is locked out.
Login Monitor	Allows viewing of list of currently logged in users, and receives automatic notifications of user login activity for users logged in through TL1 or CTC. User sessions that are idle beyond a set time associated with their privilege level are locked out.
Identification & Authentication (I&A) Mechanism	Enforces individual I&A in conjunction with group/role based I&A mechanisms, and provides centralized strong authentication mechanism; and users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE.

2.4 Features Outside of Scope

Current software and hardware features outside the scope of the TSF and thus not evaluated are:

Non-security related alarm functions
Fan tray and LCD control
Lamp test and power monitoring
Cross-connect and transport interface functions
System availability functionality (e.g. redundant TCC2 card)

SNMP management
Remote management

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

3.1 Secure Usage Assumptions

The following assumptions relate to the operation of the TOE:

Table 3 – Secure Usage Assumptions

Name	Description
A.NOEVIL	Administrators of the TOE are assumed to be non-hostile and trusted to perform their duties in a secure manner.
A.PHYSICAL	Appropriate physical security controls, such as locating the TOE(s) in a secure communications room, securing the trusted NTP server, and the DCC links must be implemented to protect the ONS 15454 installation from unauthorized access and modification.
A.PERSONNEL	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.TIMESOURCE	Clock sources external to the scope of the TOE are assumed to be in a secure location so as to provide a trusted clock source for the TOE's internal clock. This includes the TOE's real time clock (RTC) or the trusted Network Time Protocol (NTP) server located on a trusted network.
A.TRUSTEDNET	The TOE must be located within an organization's secure management network which is physically secure, and management and configuration of the TOE are: initiated from a management workstation connected to the trusted network and protected using TOE security functions and OSPs, thus only permitting access to Trusted TOE administrators. The trusted management network will contain the NTP server, and DCC links.

Name	Description
A.NODCCCONNECTIONS	ONS 15454 DCC connections are only made to other ONS 15454's in the CC-evaluated configuration. The DCC link will be afforded appropriate protection by the Network owner such that data cannot be accessed in transit between network nodes.

3.2 Threats to Security

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats Addressed by the TOE

The TOE addresses the following threats:

Table 4 – Threats countered by the TOE

Name	Description
T.USERATTACK	An unauthorized individual may gain access to the TOE and compromise its security functions by altering its configuration and/or data.
T.APPATTACK	An unauthorized process or application may gain access to the TOE and compromise its security functions by altering its configuration and/or data.
T.EXCEEDPRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in the illegal modification of the TOE configuration and/or data.
T.NORESPONSE	A pre-defined security alarm event monitored by the TOE is detected and fails to alert the administrator.
T.NODETECT	An unauthorized user, process or application attempts to mount an attack against the TOE security functions and/or associated data, which succeeds without detection.

3.2.2 Threats Addressed by the Operating Environment

There are no threats addressed by the TOE operational environment.

3.3 Organizational Security Policies

The table following describes the organizational security policies relevant to the operation of the TOE.

Table 5 – Organizational Security Policies

Name	Description
P.RESPOND	The organization shall respond in a timely fashion to alarms generated by the TOE in accordance with a defined security policy covering the secure administration of the TOE.
P.PERSONNEL	The organization shall have in place policies, training programs, and reporting and enforcement mechanisms such that personnel know their security responsibilities (or role) when using the TOE.

4 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the ST, is to be addressed. Just as some threats are to be addressed by the TOE and others by its intended environment, some security objectives are for the TOE and others are for its environment. These two classes of security objectives are discussed separately.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as described in the following table.

Table 6 – Security Objectives for the TOE

Name	Description
O.SECURE_OPERATE	The TOE shall prevent unauthorized changes to its security functions, configuration and associated data.
O.MONITOR	The TOE shall provide the capability to monitor and control user sessions.
O.SECURE_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to the security functions, configuration and associated data.
O.PRIVILEGE	The TOE shall ensure that authorized users do not exceed their assigned privileges.
O.AUDIT	The TOE shall record the necessary events to ensure that all users of the TOE are held accountable for their actions.

4.2 Security Objectives for the Environment

The security objectives for the TOE environment are as described in the following table.

Table 7 – Security Objective for the Environment

Name	Description
OE.PHYSICAL	The TOE environment shall control access to the facility where the TOE is located to prevent unauthorized physical access.
OE.SECURE_MANAGE	The TOE environment shall ensure that the management of the TOE is performed in a secure manner by trusted personnel.

Name	Description
OE.TRAINING	The TOE environment shall ensure that administrators are trained to make the right choices when providing administrative support to the TOE, and that operators and users are trained to operate and use the TOE in a secure fashion.
OE.NTP_SERVER	The TOE environment shall ensure that a trusted and reliable NTP server is available to periodically synchronize the TOE's internal system clock with the NTP server.
OE.SECURE_ACCESS	The TOE environment shall support secure communications and ensure that only those authorized users and applications are granted access to the security functions, configuration and associated data that is transmitted between two TOEs.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in summary form in the table below.

Table 8 – TOE Security Functional Requirements

No.	Component	Component Name
Class FAU: Audit		
	FAU_AUD.1	Audit data generation
	FAU_SAR.1	Security audit review
Class FDP:	**User Data Protection**	
	FDP_ACC.1	Access control policy
	FDP_ACF.1	Security attribute based access control
Class FIA: Identification and Authentication		
	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Class FMT: Security Management		
	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FMT_SMR.3	Assuming roles
Class FPT: Protection of the TSF		
	FPT_SEP.1	TSF Domain Separation
	FPT_STM.1	Reliable Time Stamps
Class FTA: TOE Access		
	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_TSE.1	TOE session establishment

No.	Component	Component Name
	FTA_SSL.3	TSF-initiated termination

The following sections contain the functional components derived from the Common Criteria Part 2 [CC2], with the exception of FAU_AUD.1. Please note that it was necessary to create FAU_AUD.1 (modeled on FAU_GEN.1) in order to make it more representative of the audit capability implemented by the TOE (refer to section 8.4 for further information).

The standard CC text is in regular font; the text inserted by the Security Target (ST) author is in accordance with the conventions described in at the beginning of this document.

5.1.1 Security Audit (FAU)

Audit data generation (FAU_AUD.1)

Hierarchical to: No other components.

FAU_AUD.1.1 **The TSF shall be able to generate an audit record of the following auditable events for HTTP, CTC and TL1:**

a) All auditable events for the *not specified* level of audit; and [

b) Successful and unsuccessful user login attempts;

c) User logout;

d) User lockout when the default number of login attempts has been exceeded;

e) Forced user logout initiated by superuser;

f) User creation and deletion; and

g) User privilege level modification].

FAU_AUD.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 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 ST.

Dependencies: FPT_STM.1 Reliable time stamps

Security Audit Review (FAU_SAR.1)

Hierarchical to: No other components.

FAU_SAR.1.1	The TSF shall provide [Superuser] with the capability to read [all audit information] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit Data Generation

5.1.2 User Data Protection (FDP)

Subset Access Control (FDP_ACC.1)

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [access control SFP] on [Subject: All users Objects: System date and time, DCC links, system database, audit logs, node attributes and all account attributes Operations: All user actions].
Dependencies:	FDP_ACF.1 Security Attribute Based Access Control

Access Control Functions (FDP_ACF.1)

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following [Subject: All users Objects: System date and time, DCC links, system database, audit logs, node attributes and all account attributes Security Attribute: Privilege Level].
FDP_ACF.1.2	The TSF shall enforce the following rules **specified in Table 10 – Access Control Permissions** to determine if an operation among controlled subjects and controlled objects is allowed.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [*no additional explicit denial rules*].
Dependencies:	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization

Table 9 – Access Control Permissions

Object	Object Description	Actions	Privilege Level Required			
			Retrieve	Maintenance	Provisioning	Superuser
Audit logs	Alarms	Synchronize/filter /delete cleared alarms	X	X	X	X
	Conditions	Retrieve/filter	X	X	X	X
	Session History	Filter and Search	X	X	X	X
	Node History	Retrieve alarms and events/filter/search	X	X	X	X
	System Audit Log	Retrieve				X
Account Attributes	User Account Attributes	Users: create/change/delete				X
		Change password	(Same user)	(Same user)	(Same user)	(All users)
		Active logins: logout				X
		Policy: change				X
Node Attributes	SNMP Attributes	Create/delete/edit			X	X
	Network Element Defaults	Edit				X
	Alarm attributes	Set security thresholds and clear security alarms				X
		Edit behavior			X	X
DCC Links	DCC	Create/edit/delete			X	X
System Date & Time	Date & Time Settings	Set date and time, configure NTP/SNTP settings			X	X
System Database	Database	Backup		X	X	X
		Restore				X

Object	Object Description	Actions	Privilege Level Required			
			Retrieve	Maintenance	Provisioning	Superuser
	Software	Upgrade/activate/ revert				X

5.1.3 Identification and Authentication (FIA)

Authentication Failure Handling (FIA_AFL.1)

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when the Superuser defined [1-10 inclusive, **for HTTP/CTC, and TL1**] unsuccessful authentication attempts occur related to following authentication events:

- [incorrect password].

FIA_AFL.1.2 When the Superuser defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock out user access].

Dependencies: FIA_UAU.1 Timing of authentication.

User Attribute Definition (FIA_ATD.1)

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,
- Privilege Level
- Last Login Time,
- Last Login Node,
- Failed Logins, and
- Locked Out status].

Dependencies: No dependencies.

User Authentication before any Action (FIA_UAU.2)

Hierarchical to: FIA_UAU.1

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

User Identification before any Action (FIA_UID.2)

Hierarchical to:	FIA_UID.1
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.

5.1.4 Security Management (FMT)

Management of Functions in the TSF (FMT_MOF.1)

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to *determine the behavior of, disable, enable, **and** modify the behavior of* the functions [that control user privileges, session control and monitoring parameters] to [Superuser].
Dependencies:	FMT_SMR.1 Security Roles

Management of Security Attributes (FMT_MSA.1)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [access control SFP] to restrict the ability to *query, modify **and** delete* the security attributes [TSF data] to [Superuser].
Dependencies:	FDP_ACC.1 Subset Access Control FMT_SMR.1 Security Roles

Static Attribute Initialization (FMT_MSA.3)

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [Superuser] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of Security Attributes FMT_SMR.1 Security Roles

Management of TSF Data (FMT_MTD.1)

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to *query, modify, delete **and** clear* the [TSF configuration] to [Superuser].

Dependencies: FMT_SMR.1 Security Roles

Specification of Management Functions (FMT_SMF.1)

Hierarchical to: No other components.

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

- [Modify user accounts;
- Assign privilege levels;
- Set security parameters, such as, allowable number of failed login attempts; and
- Logout another user].

Dependencies: No Dependencies

Security Roles (FMT_SMR.1)

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles: [Superuser, Provisioning, Maintenance, Retrieve].

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

Dependencies: FIA_UID.1 Timing of Identification

Assuming Roles (FMT_SMR.3)

Hierarchical to: No other components.

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [Superuser].

Dependencies: FMT_SMR.1 Security Roles

5.1.5 Protection of the TSF (FPT)

TSF Domain Separation (FPT_SEP.1)

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for is own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies:	No dependencies.

Reliable Time Stamps (FPT_STM.1)

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies:	No dependencies.

5.1.6 TOE Access (FTA)

Basic Limitation on Multiple Concurrent Sessions (FTA_MCS.1)

Hierarchical to:	No other components.
FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of [one] session per user **on a given node to a single session each**.
Dependencies:	FIA_UID.1 Timing of Identification

TSF-initiated termination (FTA_SSL.3)

Hierarchical to:	No other components.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a **period exceeding the following limits per user privilege level**: [Superuser: 15 minutes Provisioning: 30 minutes Maintenance: 60 minutes].
Dependencies:	No dependencies

TOE Session Establishment (FTA_TSE.1)

Hierarchical to:	No other components.
FTA_TSE.1.1	**For HTTP/CTC and TL.1** the- TSF shall be able to deny session establishment based on [the number of failed logins resulting in user lockout].
Dependencies:	No dependencies.

5.2 TOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements correspond to the **Evaluation Assurance Level 2** from Part 3 of the CC [CC3], and are listed in summary form in the table below.

Table 10 – TOE Security Assurance Requirements

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.2	Configuration items
Class ADO: Delivery and Operation		
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation and start-up
Class ADV: Development		
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high level design
6	ADV_RCR.1	Informal representational correspondence
Class AGD: Guidance documents		
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
Class ATE: Tests		
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing- sample
Class AVA: Vulnerability Assessment		
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

5.2.1 Configuration Management (ACM)

Configuration Items (ACM_CAP.2)

Dependencies: No dependencies

ACM_CAP.2.1D	The developer shall provide a reference for the TOE.
ACM_CAP.2.2D	The developer shall use a CM system.
ACM_CAP.2.3D	The developer shall provide CM documentation.
ACM_CAP.2.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2C	The TOE shall be labeled with its reference.
ACM_CAP.2.3C	The CM documentation shall include a configuration list.
ACM_CAP.2.4C	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7C	The CM system shall uniquely identify all configuration items.

5.2.2 Delivery and Operation (ADO)

Delivery Procedures (ADO_DEL.1)

Dependencies: No dependencies

ADO_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D	The developer shall use the delivery procedures.
ADO_DEL.1.1C	The delivery documentation shall describe all the procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Installation, Generation, and Start-Up Procedures (ADO_IGS.1)

Dependencies: No dependencies

ADO_IGS.1.1D	The developer shall document procedures necessary for the secure

	generation, and start-up of the TOE.
ADO_IGS.1.1C	The installation, generation, and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

5.2.3 Development (ADV)

Informal Functional Specification (ADV_FSP.1)

Dependencies:	No dependencies
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.

Descriptive High Level Design (ADV_HLD.1)

Dependencies:	ADV_FSP.1 Informal functional specification ADV_RCR.1 Informal correspondence demonstration
ADV_HLD.1.1D	The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1C	The presentation of the high level design shall be informal.
ADV_HLD.1.2C	The high level design shall be internally consistent.
ADV_HLD.1.3C	The high level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C	The high level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C	The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions

	provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6C	The high level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7C	The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Informal Correspondence Demonstration (ADV_RCR.1)

Dependencies:	No dependencies
ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent parts of TSF representation that are provided.
ADV_RCR.1.1C	For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely verified in the less abstract TSF representation.

5.2.4 Guidance Documents (AGD)

Administrator Guidance (AGD_ADM.1)

Dependencies:	ADV_FSP.1 Informal functional specification
AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrator personnel.
AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values, as appropriate.

AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

User Guidance (AGD_USR.1)

Dependencies:	ADV_FSP.1 Informal functional specification
AGD_USR.1.1D	The developer shall provide user guidance.
AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrator users of the System TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the System TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of the TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Tests (ATE)

Evidence of Coverage (ATE_COV.1)

Dependencies:	ADV_FSP.1 Informal functional specification ATE_FUN.1 Functional testing
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 identified in the test documentation and the TSF as described in the functional specification.

Functional Testing (ATE_FUN.1)

Dependencies:	No dependencies.
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, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each test security function behaved as specified.

Independent testing – sample (ATE_IND.2)

Dependencies:	ADV_FSP.1 Informal functional specification AGD_USR.1 User guidance ATE_FUN.1 Functional testing
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.

5.2.6 Vulnerability Assessment (AVA)

Strength of TOE Security Function Evaluation (AVA_SOF.1)

Dependencies:	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high level design
AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the SPP/SST.

Developer Vulnerability Analysis (AVA_VLA.1)

Dependencies:	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high level design AGD_USR.1 User guidance
AVA_VLA.1.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.1.2D	The developer shall provide vulnerability analysis documentation
AVA_VLA.1.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2C	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3C	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended

environment of the TOE.

5.3 Security Requirements for the IT Environment

This section contains the security functional requirements for the IT Environment.

Reliable Time Source (FPT_STM_EXP.1)

Hierarchical to:	No other components.
FPT_STM_EXP.1.1	The IT Environment shall be able to provide a reliable time source for use by the TOE time stamp function.
Dependencies:	No dependencies.

Inter-TSF Trusted Channel (FTP_ITC_EXP.1)

Hierarchical to:	No other components.
FTP_ITC_EXP.1.1	The IT Environment shall provide a communication channel between two instantiations of the TOE that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC_EXP.1.2	The IT Environment shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC_EXP.1.3	The TSF shall initiate communication via the trusted channel for: transmission of authentication parameters and other TSF from one TOE to another.
Dependencies:	No dependencies.

Application Note for FTP_ITC_EXP.1: The purpose of this SFR for the IT Environment is to support and ensure that passwords and other TSF data are not compromised during transmission between TOEs across an established Data Communications Channel (DCC) link.

TSF Domain Separation (FPT_SEP_EXP.1)

Hierarchical to:	No other components.
FPT_SEP_EXP.1.1	The IT Environment shall maintain for the TSF a security domain for execution by the TSF that protects the TSF from interference and tampering by untrusted subjects.
FPT_SEP_EXP.1.2	The IT Environment shall enforce separation between the security

domains of subjects in the TSC.

Dependencies: No dependencies.

Application Note for FPT_SEP_EXP.1: The purpose of this SFR for the IT Environment is to support and ensure that line cards of the MSPP protect the management interfaces of the TOE such that they cannot be accessed from sources external to the trusted management network.

5.4 Security Requirements for the Non-IT Environment

The TOE has no security requirements for the non-IT environment.

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation. Accordingly the TOE security functions detailed below and the SFRs identified in Section 5.1 above pertain exclusively to authorized user access using CTC, HTTP, and TL1.

6.1 IT Security Functions

This section presents the security functions implemented by the TOE.

6.1.1 Security Management (SM)

SM.ROLE – Security Management Roles

The TOE can be configured, managed and operated via direct local connection to the craft interface using CTC or TL1. Each CTC or TL1 user can be assigned one of following four (4) privilege levels (in ascending order):

- Retrieve – can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance – can access only ONS 15454 maintenance options, including the retrieval and viewing of CTC information.
- Provisioning – can access provisioning and maintenance options, including the retrieval and viewing of CTC information.
- Superusers – can perform all of the functions of the other privilege levels, including authorization to manage TSF data, which includes creating the user and privilege levels for other users.

Each privilege level has an associated set of actions that is permitted to users at that privilege level.

SM.SUPERUSER – Superuser Privilege Login

A default Superuser ID is provided with every ONS 15454, whose password should be changed at initial login. This default userid is provided to setup the ONS 15454 for initial use. The default ID has Superuser privileges, so that only the Superuser can create, or delete, other users. Initially, another Superuser must be created before the default Superuser, CISCO15 user can be deleted. The default Superuser ID is delivered without a password, and therefore a password needs to be created following the initial login. Following this initial login activity this first Superuser can then create the rest of the users. The Superuser privilege provides that level user with sole responsibility for the security of the nodes. The Superuser privilege includes the ability to view and monitor the list of logged in users, and the ability to log off and to change the privilege level of any user. Additionally, the Superuser can see failed login attempts and users who have been locked out due to exceeding the failed login attempt threshold. The Superuser privilege level can also set the number of invalid login attempts that a user can make before their ID is locked out. The locked out userid does not allow a login.

The Superuser(s) has full authority and ability to define groups and their privileges, and the Superuser has complete control over the TOE. The TOE allows the Superuser to set the length of the idle time for each privilege level, denoting the length of time allowable for the session to be idle before that session window is locked. The timeout value can be changed from the default value on both a Node and a user basis, from which the user is automatically logged out when the idle user

time exceeds the threshold value. The Superuser is able to lockout another user. Additionally, the Superuser can set the duration of the lockout to either a specified duration, or manual unlock by Superuser required.

SM.MANAGE – Security Management

Users can be provisioned by the Superuser for a single or a multiple login occurrence on a given node. The default value is to permit multiple concurrent user ID sessions on a node, which permits multiple users to log into a node using the same user ID (and password). If the default user ID privilege level is provisioned for a single occurrence, then concurrent logins to the node with the same user ID are not permitted. The default setting for each node is to allow multiple concurrent sessions. The default setting is to only allow a single concurrent login per account, per node. In addition the installer is required to change this setting from the system default in order for the product to be in the evaluated configuration. A Superuser can perform user management tasks from the network or the node (default login view). In network view, the Superuser can add, edit, or delete users from multiple nodes at one time. User management tasks in node view only enable the Superuser to add, edit, or delete users from that node.

6.1.2 Audit Trail and Security Alarm Events (AA)

AA.EVENTS - Security Events

The TOE generates a variety of security events to allow system administrators to see intrusion attempts. These will take the form transient events and Audit (Security Log) entries. An example of the former would be if an invalid user id tries to login, the activity will be sent to the CTC and the TL1 Superuser as a transient event. Transient events are intended to alert the Superuser to check out the security log. Additional security events include the number of invalid login attempts has exceeded the threshold; audit trail file is 80% full; and audit trail file is 100% full. The security log will also have Login notification (only accessible by Superusers); Threshold of Failed Login Attempts Met (Lockout); Invalid userid Login Attempted; and Intrusion Attempts (Login Failures). All security events will report a Security Event entry in the Audit Log that will be viewable only on Audit Retrievals by Superusers. As an example, an invalid userid login attempts (invalid userid, rather than valid id and invalid password) shall raise and log a security event; and the log will record an invalid access attempt with invalid userid and IP address from the node which the attempt occurred.

AA.AUDIT – Audit Trail

TOE audit retrieval will get all audit records including the following security related entries:

1. Login
2. Logout
3. Login Failure
4. Lockout (threshold of Login Failures met)
5. forced session logout initiated by Superuser
6. User Creation
7. User Deletion
8. User Privilege level modification.

The TOE maintains a 640-entry, human readable audit trail of user actions such as login, logout, and creation or deletion of DCC links between two TOEs. The Audit Log can be stored for later

review and analysis. Any violation of a security threshold generates an alarm and the alarm event is recorded. Each audited event contains a date and timestamp for that event (see Section 5.1.1 FAU_AUD.1.2). The audit trail can be archived via CTC, in which the back-up/archives all records not backed up since the last archive operation to a local file. The archive files provide a view of the node's audit travel over time without omissions or overlap.

6.1.3 Login Control and Monitor (CM)

CM.CONTROLS - Login Controls

TOE Login Controls includes the ability to limit the number of failed login attempts per node and per user (between 1 and 10). TOE Login Controls supports up to 20 sessions. When a username has reached the threshold number of failed login attempts, that username will be locked out. Lockout duration can be set to Infinite, or be settable from 0 to 600 seconds. "Zero" means the feature is disabled and "Infinite" means a Superuser has to manually reset the user so he can login. A lockout causes a security event to be reported and logged. The audit file will contain the username and the IP address of the locked out client. The username in the Lockedout state cannot login, even when a valid password for that user is entered. Additionally, an exception will be reported for any login attempts by locked out usernames that try subsequent logins. Allows viewing of list of currently logged in users, and receives automatic notifications of user login activity for users logged in through TL1 or CTC.

CM.MONITOR – Monitor User Sessions

Login notifications allow the Superuser to know who is working with which nodes. A notification will be generated automatically for user login activity (login/logout). A Superuser will have the ability to logout a user that is currently logged into a node. Additionally, the Superuser will be able to change the privilege level for any user that is logged on, which will then take effect at the next user login for that particular user. Additionally, session idle timeout periods can be provisioned and monitored, such that when session inactivity has reached the timeout threshold, then that user is locked out.

6.1.4 Identification and Authentication (IA)

IA.MECHANISM – Identification & Authentication Mechanism

The TOE enforces individual identification and authentication (I&A) in conjunction with group/role based I&A mechanisms, and provides a centralized authentication mechanism. Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE, whether those actions are management of user accounts or the configuration of routes. The TOE requires that applications exchanging information with the TOE to successfully authenticate prior to any exchange.

6.1.5 Self-Protection of the TOE (SP)

SP.TIMESOURCE – Reliable Time Source

The TOE implements a real time clock on the TCC2. This time source provides the time-stamping mechanism for the auditing functions of the TOE. The time source has been designed to provide a trusted and reliable reference for supporting the time-related functions of the TOE. The time itself

may either be set manually by the Superuser or Provisioner, or synchronized via a NTP/SNTP server.

SP.DOMAIN – Domain Separation

The TOE is an appliance in which all operations are self-contained, with all administration and configuration operations performed within the physical boundary of the TOE. The TOE has been designed so that all user and router data can only be manipulated via the CTC/TL1 interface. This design, combined with the fact that, with the exception of clock set, only a user with the Superuser privilege level may access the TOE security functions, provides a distinct protected domain for the TSF.

6.2 Assurance Measures

The TOE claims to satisfy the assurance requirements for the Common Criteria Evaluation Assurance Level EAL2 (CC EAL2). This section identifies the Configuration Management, System Development Procedures, System Test Documentation and System Installation and Guidance Documentation measures applied by TOE to satisfy the CC EAL2 assurance requirements defined in the CC Part3 [CC3].

Table 11 - Assurance Measures

Assurance Measure Label	Assurance Measure Description
CM_DOC	Configuration management documentation that includes a configuration list, a description of the configuration items comprising the TOE and a description of the method used to uniquely identify the configuration items. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Configuration Management Documentation
DEL_DOC	Delivery documentation that describes all procedures necessary to maintain security for distribution of the TOE to a user's site. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Delivery Procedure
IGS_DOC	Installation and generation documentation that describes the steps necessary for secure installation, generation and startup of the TOE. Evidence title(s): Installation and Configuration Guide for the Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3
FUN_SPEC	Functional specification that describes the TSF and its external interfaces and the purpose and method of use of external TSF interfaces, including details of effects, exceptions and error messages. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Functional Specification
HLD_DOC	High-level design that describes the structure of the TSF in terms of sub-systems and describes the security functionality provided by each sub-system.

Assurance Measure Label	Assurance Measure Description
	Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 High Level Design
RCR_DOC	Representation correspondence analysis that, for each adjacent pair TSF representations, demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Functional Specification
ADMIN	Administrator guidance that describes the administrative functions and interfaces available to the administrator of the TOE, describes how to administer the TOE in a secure manner, describes warnings about functions and privileges that should be controlled in a secure processing environment, describes all assumptions about user behavior relevant to secure operation, describes all security parameters under the control of the administrator, and describes each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. Evidence title(s): Installation and Configuration Guide for the Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3
USER	User guidance that describes the functions and interfaces available to the non administrative users of the TOE, describes the use of user accessible security functions, describes warnings about user accessible functions and privileges that should be controlled in a secure processing environment, and describes all user responsibilities necessary for secure operation of the TOE. Evidence title(s): All users are administrators
TEST_COV	Test evidence that shows the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Test Coverage Analysis
TEST_DOC	Test documentation consisting of test plans, test procedure descriptions, expected test results and actual test results. The test plan identifies the security functions to be tested and the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. The expected test results show the anticipated outputs from successful test execution. The actual test results demonstrate that each tested security function behaved as specified. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Functional Test Results and Analysis
VLA_DOC	A vulnerability analysis that shows that for all identified vulnerabilities, the vulnerability cannot be exploited in the intended environment of the TOE. For each mechanism identified in the Security Target, an analysis shows that the claimed strength of TOE security function meets or exceeds the minimum strength level

Assurance Measure Label	Assurance Measure Description
	defined in the Security Target. Evidence title(s): Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Vulnerability Analysis

7 PP Claims

This Security Target does not claim conformance to a PP.

8 Rationale

8.1 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are suitable, that is they are sufficient to address the security needs, and that they are necessary, i.e., there are no redundant security objectives.

8.1.1 All Assumptions, Threats and Policies Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (Table 12) shows that all of the secure usage assumptions, threats to security, and organizational security policies have been addressed.
- The second section (Table 13) shows that each security objective counters at least one assumption, policy, or threat.

Table 12 - Mapping of Assumptions, Threats, and OSPs to Security Objectives

Threat/Policy/Assumption Label	Associated Security Objective
A.NOEVIL	OE.SECURE_MANAGE
A.PHYSICAL	OE.PHYSICAL OE.SECURE_ACCESS
A.PERSONNEL	OE.TRAINING
A.TIMESOURCE	OE.NTP_SERVER
A.TRUSTEDNET	OE.PHYSICAL OE.SECURE_ACCESS
A.NODCCCONNECTION	OE.SECURE_MANAGE OE.PHYSICAL
T.USERATTACK	O.SECURE_OPERATE O.SECURE_ACCESS O.PRIVILEGE
T.APPATTACK	O.SECURE_OPERATE O.SECURE_ACCESS
T.EXCEEDPRIV	O.PRIVILEGE O.AUDIT O.SECURE_OPERATE

Threat/Policy/Assumption Label	Associated Security Objective
T.NORESPONSE	O.MONITOR O.AUDIT
T.NODETECT	O.MONITOR O.AUDIT
P.RESPOND	O.MONITOR OE.TRAINING
P.PERSONNEL	O.PRIVILEGE OE.TRAINING

Table 13 shows that there are no unnecessary IT security objectives.

Table 13 - Mapping of Security Objectives to Threats, Policies and Assumptions

Objective Label	Threat / Policy/ Assumption
O.SECURE_OPERATE	T.USERATTACK T.APPATTACK T.EXCEEDPRIV
O.MONITOR	T.NORESPONSE T.NODETECT P.RESPOND
O.SECURE_ACCESS	T.USERATTACK T.APPATTACK
O.PRIVILEGE	T.USERATTACK T.EXCEEDPRIV P.PERSONNEL
O.AUDIT	T.EXCEEDPRIV T.NORESPONSE T.NODETECT
OE.PHYSICAL	A.PHYSICAL A.TRUSTEDNET O.NODCCCONNECTION

Objective Label	Threat / Policy/ Assumption
OE.SECURE_MANAGE	A. NOEVIL A.NODCCCONNECTION
OE.TRAINING	A.PERSONNEL P.RESPOND P.PERSONNEL
OE.NTP_SERVER	A.TIMESOURCE
OE.SECURE_ACCESS	A.PHYSICAL A.TRUSTEDNET

8.1.2 Security Objectives are Sufficient

The following arguments are provided in
Table **14** to demonstrate the sufficiency of the Security Objectives outlined above.

Table 14 - Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to support Security Objective sufficiency
A.NO_EVIL	This assumption is upheld by the following security objective: ▪ OE.SECURE_MANAGE ensures that only trusted TOE administrators manage the TOE in a secure manner so that the integrity and confidentiality of the TOE and its associated data is maintained.
A.PHYSICAL	This assumption is upheld by the security objective: • OE.PHYSICAL, which ensures that the TOE is located in a physically secure environment • OE.SECURE_ACCESS ensures that the TOE environment supports secure communications and that only those authorized users and applications are granted access to the security functions, configuration and associated data that is transmitted between two TOEs.
A.PERSONNEL	This assumption is upheld by the following security objective: ▪ OE.TRAINING as the personnel operating the TOE will be trained in doing so in a secure manner.
A.TIMESOURCE	This assumption is upheld by the security objective OE.NTP_SERVER, which ensures that a trusted and reliable NTP server is available to periodically synchronize the TOE's internal

Assumption/Threat/Policy	Argument to support Security Objective sufficiency
	system clock with the NTP server.
A.TRUSTEDNET	This assumption is upheld by the following security objective: ▪ OE.PHYSICAL ensures that the TOE is situated in a physically secure location as to minimize the opportunity of direct attack ▪ OE.SECURE_ACCESS ensures that the TOE environment supports secure communications and that only those authorized users and applications are granted access to the security functions, configuration and associated data that is transmitted between two TOEs.
A.NODCCCONNECTION	This assumption is upheld by the following security objectives: • OE.SECURE_MANAGE ensures that only trusted TOE administrators manage the TOE in a secure manner so that the integrity and confidentiality of the TOE and its associated data is maintained. • OE.PHYSICAL ensures that the TOE is situated in a physically secure location as to minimize the opportunity of direct attack
T.USERATTACK	The threat of a user-initiated attack on the TOE is countered by the following security objectives: ▪ O.SECURE_OPERATE ensures that any changes initiated from a user who has not been authorized will not succeed ▪ O.SECURE_ACCESS ensures that only those users who have been granted access to the TOE are able to modify the TOE security functions and configuration data ▪ O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned privilege
T.APPATTACK	The threat of a process or application-initiated attack on the TOE is countered by the following security objectives: ▪ O.SECURE_OPERATE ensures that any changes initiated from an application or process that has not been authorized will not succeed ▪ O.SECURE_ACCESS ensures that only those applications that have been granted access to the TOE are able to modify the TOE security functions and configuration data
T.EXCEEDPRIV	The threat of an authorized user exceeding his/her privileges and subsequently illegally modifying the TOE configuration is countered by the following security objectives: ▪ O.PRIVILEGE ensures that the user is only permitted to perform the security functions corresponding to their assigned

Assumption/Threat/Policy	Argument to support Security Objective sufficiency
	privilege ▪ O.SECURE_OPERATE ensures that any changes initiated from a user who has not been authorized (and therefore does not have the appropriate privilege) will not succeed ▪ O.AUDIT provides for the recording of security-relevant events and associating users (and their privileges) with those events
T.NORESPONSE	The threat of a monitored user-level security event failing to alert the TOE administrator is countered by the following security objectives: ▪ O.MONITOR ensures that the TOE has implemented the necessary security functions to monitor and control user sessions. ▪ O.AUDIT provides for the recording of security-relevant events viewable by an administrator whom may then decide to respond to suspicious events
T.NODETECT	The threat of an attack on the TOE security functions by an unauthorized user, application or process succeeding and going undetected by the TOE is countered by the combination of both security objectives: ▪ O.MONITOR ensures that the TOE has implemented the necessary security functions to monitor and control user sessions, so that an attack originating from a user will be detected ▪ O.AUDIT ensures that all security-relevant events (originating from either a user, process, or application) that may indicate an attack on the TOE security functions are recorded and that information recorded is sufficient to hold users accountable for their security-relevant actions
P.RESPOND	The OSP requirement for a timely response to a security alarm is met by the following security objectives: ▪ O.MONITOR as the effectiveness of responding to user-level security events is dependant on administrator's training and awareness of the policies relevant to the actions required when responding to events and alarms raised by the TOE ▪ OE.TRAINING as the staff operating the TOE will be trained in doing so in a secure manner.
P.PERSONNEL	The OSP requirement for having the appropriate policies, training programs etc in place such that personnel know their security responsibilities is met by the following security objectives: ▪ O.PRIVILEGE as each user of the TOE should be aware of the security functions they are allowed to access as determined by their privilege level allocated by the TOE ▪ OE.TRAINING as the staff operating the TOE will be trained

Assumption/Threat/Policy	Argument to support Security Objective sufficiency
	in doing so in a secure manner.

8.2 Security Requirements Rationale

8.2.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are suitable to meet the security objectives. Table 15 and Table 16 show that each security requirement is necessary, that is, each security objective is addressed by at least one security requirement and vice versa.

Security objectives for the TOE are satisfied by the TOE security functional requirements. Security objectives for the environment are satisfied by the requirements for the non-IT environment.

Table 15 - Mapping of Security Objectives to Security Requirements

Security Objectives	Security Requirements
O.SECURE_OPERATE	FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FPT_SEP.1, FTA_SSL.3
O.MONITOR	FAU_AUD.1, FAU_SAR.1, FIA_AFL.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FTA_MCS.1, FTA_SSL.3, FTA_TSE.1
O.SECURE_ACCESS	FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3, FPT_SEP.1, FTA_MCS.1, FTA_SSL.3, FTA_TSE.1
O.PRIVILEGE	FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3
O.AUDIT	FAU_AUD.1, FAU_SAR.1, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FPT_STM.1

Table 16 - Mapping of Security Requirements to Security Objectives

Security Requirements	Security Objectives
FAU_AUD.1	O.MONITOR, O.AUDIT

Security Requirements	Security Objectives
FAU_SAR.1	O.MONITOR, O.AUDIT
FDP_ACC.1	O.SECURE_OPERATE, O.SECURE_ACCESS, O.PRIVILEGE
FDP_ACF.1	O.SECURE_OPERATE, O.SECURE_ACCESS, O.PRIVILEGE
FIA_AFL.1	O.MONITOR, O.SECURE_ACCESS
FIA_ATD.1	O.SECURE_OPERATE, O.SECURE_ACCESS, O.PRIVILEGE
FIA_UAU.2	O.SECURE_ACCESS, O.AUDIT
FIA_UID.2	O.SECURE_ACCESS, O.AUDIT
FMT_MOF.1	O.SECURE_OPERATE, O.MONITOR, O.SECURE_ACCESS, O.PRIVILEGE, O.AUDIT
FMT_MSA.1	O.SECURE_OPERATE, O.MONITOR, O.SECURE_ACCESS, O.PRIVILEGE
FMT_MSA.3	O.SECURE_OPERATE, O.MONITOR, O.SECURE_ACCESS, O.PRIVILEGE
FMT_MTD.1	O.SECURE_OPERATE, O.SECURE_ACCESS, O.PRIVILEGE
FMT_SMF.1	O.SECURE_OPERATE, O.MONITOR, O.SECURE_ACCESS, O.PRIVILEGE
FMT_SMR.1	O.SECURE_ACCESS, O.PRIVILEGE
FMT_SMR.3	O.SECURE_ACCESS, O.PRIVILEGE
FPT_SEP.1	O.SECURE_OPERATE, O.SECURE_ACCESS
FPT_STM.1	O.AUDIT
FTA_MCS.1	O.MONITOR, O.SECURE_ACCESS
FTA_TSE.1	O.MONITOR, O.SECURE_ACCESS,
FTA_SSL.3	O.SECURE_OPERATE, O.MONITOR, O.SECURE_ACCESS
FPT_STM_EXP.1	OE.NTP_SERVER

Security Requirements	Security Objectives
FPT_ITC_EXP.1	OE.SECURE_ACCESS
FPT_SEP_EXP.1	OE.SECURE_ACCESS

8.2.2 Sufficiency of the Security Requirements

The following table shows that security requirements are sufficient to satisfy the TOE security objectives, whether in a principal or supporting role.

Table 17 - Sufficiency of Security Requirements

Objectives	Argument to support sufficiency of Security Requirements
O.SECURE_OPERATE	The objective to prevent unauthorized changes to the TOE security functions and configuration data is met by the following security requirements: ▪ FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled to prevent unauthorized modification ▪ FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions and configuration data is based on the user privilege level (and associated allowable actions) ▪ FIA_ATD.1 associates the user privilege level with their user identity to ensure that only authorized changes to the TOE are permitted ▪ FMT_MOF.1 requires that the ability to manage the security functions that control user privileges, session control and monitoring parameters is restricted to privileged administrators. ▪ FMT_MSA.1 specifies that only privileged administrators can manage the TOE security functions and related configuration data ▪ FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE ▪ FMT_MTD.1 specifies that only privileged administrators can manage the TOE configuration ▪ FPT_SEP.1 ensures that the a separate execution domain is maintained by the TOE to avoid intentional (or otherwise) tampering with the TOE security functions and configuration data by un-trusted agents ▪ FTA_SSL.3 ensures the termination of a user session in order to mitigate session hijacking of a privileged user terminal left unattended
O.MONITOR	The objective to ensure that the TOE provides the capability to monitor and control user sessions is met by the following security requirements:

Objectives	Argument to support sufficiency of Security Requirements
	▪ FAU_AUD.1 requires the capability to generate records of security-relevant events, which can be used to monitor user sessions and investigate suspicious activity ▪ FAU_SAR.1 requires that authorized users will have the capability to read and interpret data stored in the audit logs such that security breeches can be traced to user sessions ▪ FIA_AFL.1 requires that the TOE monitor the number of failed login attempts and lock out a user if a pre-determined threshold has been reached ▪ FMT_MOF.1 supports this objective by giving the privileged administrator the ability to manage the security functions that control user privileges, session control and monitoring parameters ▪ FMT_MSA.1 supports this objective by allowing privileged administrators to manage the TOE security functions that control and monitor user sessions ▪ FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy and control user sessions ▪ FMT_SMF.1 supports the security management functions relevant to the TOE, including the configuration of control and user monitoring parameters ▪ FTA_MCS.1 restricts the maximum number of concurrent single user sessions so that the number of user sessions can be controlled ▪ FTA_SSL.3 ensures the termination of a user session after a pre-determined time period has elapsed ▪ FTA_TSE.1 will deny a user permission to establish a session after a pre-determined number of failed login attempts
O.SECURE_ACCESS	The objective to ensure that only those users and applications are granted access to the TOE security functions and configuration data is met by the following security requirements: ▪ FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled ▪ FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions and configuration data is based on the user privilege level (and allowable actions) ▪ FIA_ATD.1 associates the user privilege level with their user identity which is used authorize user access to the TOE ▪ FIA_AFL.1 requires that the TOE detect a pre-determined number of failed login attempts (and subsequently lock out that user from using the TOE) as to prevent unauthorized access to the TOE ▪ FIA_UAU.2 and FIA_UID.2 provide support for meeting this objective by requiring identification and authentication of all users

Objectives	Argument to support sufficiency of Security Requirements
	prior to gaining access to the TOE ▪ FMT_MOF.1 requires that the ability to access the security functions that control user privileges, session control and monitoring parameters is restricted to privileged administrators. ▪ FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data ▪ FMT_MSA.3 ensures that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE ▪ FMT_MTD.1 specifies that only privileged administrators can access the TOE configuration ▪ FMT_SMF.1 details the security management functions relevant to the TOE, including the configuration of access control parameters ▪ FMT_SMR.1 requires that the TOE be able to recognize the roles and to be able to associate users with their roles to facilitate the control of user access to the TOE ▪ FMT_SMR.3 requires that an explicit request is performed for those users assuming the role of a privileged administrator ▪ FPT_SEP.1 ensures that a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE ▪ FTA_MCS.1 restricts the maximum number of concurrent single user sessions so that a malicious user (for example) is restricted to a finite number of entry points (or access) into the TOE ▪ FTA_SSL.3 ensures the termination a user session in order to mitigate session hijacking of a privileged user terminal left unattended ▪ FTA_TSE.1 will deny a user permission to establish a session after a pre-determined number of failed login attempts
O.PRIVILEGE	The objective to ensure that authorized users do not exceed their privileges is met by the following security requirements: ▪ FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled ▪ FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions and configuration data is based on the user privilege level (and allowable actions) ▪ FIA_ATD.1 associates the user privilege level with their user identity which then determines the user's privileges ▪ FMT_MOF.1 requires that the ability to access the security functions that control user privileges, session control and monitoring parameters is restricted to administrators with "Superuser" privilege ▪ FMT_MSA.1 specifies that only administrators with "Superuser"

Objectives	Argument to support sufficiency of Security Requirements
	privilege can access the TOE security functions and related configuration data ▪ FMT_MSA.3 supports FDP_ACF.1 by ensuring that the default values of security attributes are restrictive in nature as to enforce the security privileges assigned to each user ▪ FMT_MTD.1 specifies that only administrators with "Superuser" privilege can access the TOE configuration ▪ FMT_SMF.1 details the security management functions relevant to the TOE, including the configuration of user privileges ▪ FMT_SMR.1 requires that the TOE be able to recognize the roles and to be able to associate users with their roles which correspond to their assigned privileges ▪ FMT_SMR.3 requires that an explicit request is performed for those users assuming the role of an administrator with the "Superuser" privilege
O.AUDIT	The objective to provide the means of detecting and recording security relevant events is met by the following security requirements: ▪ FAU_AUD.1 requires the capability to generate records of security-relevant events, including the identity of the user responsible in order to be able to hold a user accountable for their actions ▪ FAU_SAR.1 requires that authorized users will have the capability to read and interpret data stored in the audit logs such that security breeches can be detected ▪ FIA_UAU.2 and FIA_UID.2 together support FAU_AUD.1 by requiring the TOE to enforce identification and authentication of all users ▪ FMT_MOF.1 requires that that the ability to manage the audit functions be restricted to privileged administrators. ▪ FMT_SMF.1 supports the security management functions relevant to the TOE, including the configuration of control and user monitoring parameters ▪ FPT_STM.1 requires the provision of reliable time stamps that can be associated with security-relevant events
OE.PHYSICAL	The objective to ensure that the TOE environment shall control access to prevent unauthorized physical access is met by the A.PHYSICAL, as it assumes the TOE to be located within a controlled access facility that will prevent unauthorized physical access.
OE.SECURE_MANAGE	The objective to ensure that the TOE environment provide measures for secure management is met by the A.NOEVIL and A.TRUSTEDNET, which assumes that the management of the TOE is performed in a secure manner.

Objectives	Argument to support sufficiency of Security Requirements
OE.TRAINING	The objective to ensure that the TOE environment provide measures to ensure that the TOE is operated by trusted and trained staff is met by the A.PERSONNEL, as it assumes that administrators are trained and motivated to make the right choices when providing administrative support to the TOE, and that operators and users are trained and motivated to operate and use the TOE in a secure fashion.
OE.NTP_SERVER	FPT_STM.EXP.1 The objective to ensure that the TOE environment use a trusted and reliable NTP server is met by the security requirement OE.NTP_SERVER which ensures that a trusted and reliable NTP server is available to periodically synchronize the TOE's internal system clock.
OE.SECURE_ACCESS	FPT_ITC_EXP.1 The objective to support and ensure that passwords and other TSF data are not compromised during transmission between TOEs across an established Data Communications Channel (DCC) link. FPT_SEP_EXP.1: The objective to support and ensure that line cards of the MSPP protect the management interfaces of the TOE such that they cannot be accessed from sources external to the trusted management network.

8.2.3 Satisfaction of Dependencies

Table 18 shows the dependencies between the functional and assurance requirements. All of the dependencies are satisfied.

Note that (H) indicates that the dependency is satisfied through the inclusion of a component that is hierarchical to the one required.

Table 18 - Dependency Analysis

Component Reference	Requirement	Dependencies	Mapping
Functional Requirements			
1.	FAU_AUD.1	FPT_STM.1	17
2.	FAU_SAR.1	FAU_AUD.1	1
3.	FDP_ACC.1	FDP_ACF.1	4
4.	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	3, 11
5.	FIA_AFL.1	FIA_UAU.1	7 (H)
6.	FIA_ATD.1	None	-
7.	FIA_UAU.2	FIA_UID.1	8 (H)

Component Reference	Requirement	Dependencies	Mapping
8.	FIA_UID.2	None	-
9.	FMT_MOF.1	FMT_SMR.1	14
10.	FMT_MSA.1	FDP_ACC.1, FMT_SMR.1	3, 14
11.	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	10, 14
12.	FMT_MTD.1	FMT_SMR.1	14
13.	FMT_SMF.1		
14.	FMT_SMR.1	FIA_UID.1	8 (H)
15.	FMT_SMR.3	FMT_SMR.1	14
16.	FPT_SEP.1	None	-
17.	FPT_STM.1	None	-
18.	FTA_MCS.1	FIA_UID.1	8 (H)
19.	FTA_SSL.3	None	-
20.	FTA_TSE.1	None	-
Assurance Requirements			
21.	ACM_CAP.2	None	-
22.	ADO_DEL.1	None	-
23.	ADO_IGS.1	AGD_ADM.1	27
24.	ADV_FSP.1	ADV_RCR.1	26
25.	ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	24, 26
26.	ADV_RCR.1	None	-
27.	AGD_ADM.1	ADV_FSP.1	24
28.	AGD_USR.1	ADV_FSP.1	24
29.	ATE_COV.1	ADV_FSP.1, ATE_FUN.1	24, 30
30.	ATE_FUN.1	None	-
31.	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	24, 27, 28, 30

Component Reference	Requirement	Dependencies	Mapping
32.	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	24, 25
33.	AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	24, 25, 27, 28

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions Satisfy the SFRs

This section shows that each SFR is mapped to at least one IT security function and each IT security function is mapped to at least one SFR. As noted in Section 6, use of ports outside of HTTP/CTC and TL1 is disallowed, because those ports are not intended for customer use.

Table 19 - Mapping of SFRs to IT Security Functions

Security Functional Requirement	IT Security Function
FAU_AUD.1	AA.AUDIT AA.EVENTS
FAU_SAR.1	AA.AUDIT AA.EVENTS
FDP_ACC.1	SM.ROLE IA.MECHANISM
FDP_ACF.1	SM.MANAGE SM.SUPERUSER CM.CONTROLS
FIA_AFL.1	AA.AUDIT AA.EVENTS CM.MONITOR
FIA_ATD.1	SM.ROLE
FIA_UAU.2	IA.MECHANISM
FIA_UID.2	IA.MECHANISM
FMT_MOF.1	SM.SUPERUSER
FMT_MSA.1	SM.SUPERUSER
FMT_MSA.3	SM.SUPERUSER
FMT_MTD.1	SM.SUPERUSER

Security Functional Requirement	IT Security Function
FMT_SMF.1	SM.SUPERUSER
FMT_SMR.1	SM.ROLE
FMT_SMR.3	SM.ROLE SM.SUPERUSER
FPT_SEP.1	SP.DOMAIN SM.SUPERUSER
FPT_STM.1 FPT_STM_EXP.1	SP.TIMESOURCE AA.AUDIT AA.EVENTS
FTA_MCS.1	CM.CONTROLS
FTA_TSE.1	CM.CONTROLS
FTA_SSL.3	CM.MONITOR

Table 20 - Mapping of IT Security Functions to SFRs

IT Security Function	Security Functional Requirement
SM.ROLE	FDP_ACC.1 FIA_ATD.1 FMT_SMR.1 FMT_SMR.3
SM.SUPERUSER	FDP_ACF.1 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.3

IT Security Function	Security Functional Requirement
	FPT_SEP.1
SM.MANAGE	FDP_ACF.1 FTP_ITC_EXP.1
AA.EVENTS	FAU_AUD.1 FAU_SAR.1 FIA_AFL.1 FPT_STM.1
AA.AUDIT	FAU_AUD.1 FAU_SAR.1 FIA_AFL.1 FPT_STM.1
CM.CONTROLS	FDP_ACF.1 FTA_MCS.1 FTA_TSE.1
CM.MONITOR	FIA_AFL.1 FTA_SSL.3
IA.MECHANISM	FDP_ACC.1 FIA_UAU.2 FIA_UID.2
SP.DOMAIN	FPT_SEP.1 FPT_SEP_EXP.1
SP.TIMESOURCE	FPT_STM.1 FPT_STM_EXP.1

8.3.2 IT Security Function Suitability

This section provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

Table 21 - Suitability of IT Security Functions

Security Functional Requirement	Argument for suitability of IT Security Functions
FAU_AUD.1	This TOE SFR is satisfied by the Audit Trail (AA.AUDIT) and Alarm Events (AA.EVENTS) security functions by generating audit logs from the audit of a variety of security events.
FAU_SAR.1	This TOE SFR is satisfied by the Audit Trail (AA.AUDIT) and Alarm Events (AA.EVENTS) security functions by enabling the ability for only authorized users to review the audit logs.
FDP_ACC.1	This TOE SFR is satisfied by the security management roles function (SM.ROLE), which permits each user to be assigned to one of four privilege levels and the associated privileges for that privilege level. The TOE also supports a strong authentication mechanism (IA.MECHANISM) to gain access to the TOE prior to performing any security, management or operational actions.
FDP_ACF.1	This TOE SFR is satisfied by the security management (SM.MANAGE) and login control (CM.CONTROLS) security functions by permitting TOE access based on those privileges assigned for each of the four privilege levels. Additionally, the TOE Superuser (SM.SUPERUSER) has the capability to manually logout any user for unauthorized activity.
FIA_AFL.1	This TOE SFR is satisfied by the audit trail (AA.AUDIT) and security alarm event (AA.EVENTS) and login monitoring (CM.MONITOR) security functions by detecting failed login attempts and invalid userid login attempts when they exceed the threshold and by logging those event in the audit trail.
FIA_ATD.1	This TOE SFR is satisfied by the security management privilege level (SM.ROLE) security function by assigning each user to one of four privilege levels.
FIA_UAU.2	This TOE SFR is satisfied by the I&A mechanism (IA.MECHANISM) security function by requiring each user to successfully authenticate themselves using a unique identifier and password prior to performing any action on the TOE.
FIA_UID.2	This TOE SFR is satisfied by the I&A mechanism (IA.MECHANISM) security function by requiring users to successfully identify themselves using a unique identifier.

Security Functional Requirement	Argument for suitability of IT Security Functions
FMT_MOF.1	This TOE SFR is satisfied by the Superuser privilege login (SM.SUPERUSER) security function, which provides the Superuser an expanded view of the security of the nodes, which includes a list of logged-in users, and the ability to log off or change the privilege level of any user.
FMT_MSA.1	This TOE SFR is satisfied by the Superuser privilege login (SM.SUPERUSER) security function, which provides the Superuser with full authority and ability to define user groups and their privileges, complete control over the security functions of the TOE.
FMT_MSA.3	This TOE SFR is satisfied by the Superuser privilege login (SM.SUPERUSER) security function which allows the Superuser to set the number of failed login attempts, to change default settings for each node, and to allow a single login occurrence.
FMT_MTD.1	This TOE SFR is satisfied by the Superuser privilege login (SM.SUPERUSER) security function by only permitting the TOE TSF to be exclusively configured and managed by the Superuser.
FMT_SMF.1	This TOE SFR is satisfied by the Superuser privilege login function (SM.SUPERUSER) security function, via the Superuser, providing the capability to modify user accounts and access levels, set TOE security parameters, such as number of failed login attempts, and timeout durations, and enable users to login following lockout.
FMT_SMR.1	This TOE SFR is satisfied by the security management roles (SM.ROLE) security function by assigning each CTC or TL1 user to one of four privilege levels, and the privileges associated with that level.
FMT_SMR.3	This TOE SFR is satisfied by the security management roles (SM.ROLE) security function by the provision of the CISCO15 user with every ONS 15454. Only CISCO15 has Superuser privileges, so only the Superuser can create other users (SM.SUPERUSER).
FPT_SEP.1	The TOE provides protection mechanisms for its security functions, such as the restricted ability that, with the exception of clock set, only “Superusers” can perform administrative actions on the TOE (SM.SUPERUSER). Another protection mechanism is that all functions of the TOE are confined to the device itself (SP.DOMAIN). The TOE is completely self-contained, and therefore, maintains its own execution domain.
FPT_STM.1	This TOE SFR is satisfied by the internal time source (SP.TIMESOURCE) security function implemented by the TOE. It is used to ensure that each

Security Functional Requirement	Argument for suitability of IT Security Functions
	audited event contains a date and time stamp for that event.
FTA_MCS.1	This TOE SFR is satisfied by the TOE login controls (CM.CONTROLS) security function, which can support up to 20 sessions. The TOE allows each userid to be provisioned to be active for a single occurrence, which then prohibits any other userid from logging into that node. The default value is multiple concurrent sessions.
FTA_TSE.1	This TOE SFR is satisfied the login controls (CM.CONTROLS) security function by the TOE locking out a user when a username has reached the threshold number of failed login attempts. Lockout duration can be set to Infinite, or be settable from 0 to 600 seconds. "Zero" means the feature is disabled, and "Infinite" means that the Superuser has to manually reset the user so he can login. The TOE does not allow a username in the Lockedout state to login, even when a valid password for that user is entered. An exception is reported for any login attempts by locked out usernames that try subsequent logins.
FTA_SSL.1	This TOE SFR is satisfied by the monitoring (CM.MONITOR) security function by monitoring session idle timeout periods, such that when session inactivity has reached the timeout threshold, then that user is locked out. The lockouts prevent unauthorized users from making changes.

8.3.3 Demonstration of Mutual Support

The mutual supportiveness of the TOE security functional requirements and security functions can be illustrated by an analysis of those requirements that help prevent bypass, tampering, and de-activation of the SFRs. It can also be demonstrated by determining which requirements and functions enable the detection of these types of attacks and by referring to the results of the previous analyses performed in this chapter. The results of this combined analysis are presented below.

Help Prevent Bypassing of other SFRs

FIA_AFL.1, FIA_UID.2 and FIA_UAU.2 support other functions that allow user access to the assets by restricting actions that the user can take before being authorized.

The management functions FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FMT_SMR.3 support all other SFRs by restricting the ability to change security management functions to the Superuser, exclusively, ensuring that other users cannot circumvent the SFRs.

FMT_MOF.1, FMT_MSA.3, FMT_SMR.3, limit the acceptable values for secure access and security data, and protects the SFRs dependent on those values from being bypassed.

FTA_MCS.1 support other SFRs by limiting the allowable number of concurrent sessions by permitted to a user.

Help Prevent Tampering of other SFRs

FIA_UID.2 and FIA_UAU.2 support other actions that allow the user access to the TOE by restricting the actions that the user can take before being authorized.

FIA_ATD.1 a and FMT_MSA.1 support all other SFRs by restricting the ability to change privileges and associated management functions to authorized users, thus ensuring that other users cannot tamper with these SFRs.

FTA_TSE.1 and FTA_SSL.3 support all other SFRs by denying system access and session establishment by restricting unauthorized user access and session inactivity levels.

Help Prevent de-activation of other SFRs

The access control actions governed by FDP_ACC.1 and FDP_ACF.1, FTA_MCS.1 act together with other SFRs to provide control of allowed data flow, preventing unauthorized de-activation of SFRs.

FMT_MSA.1 supports all other SFRs by restricting the ability to change privileges and associated management functions to authorized users, thus ensuring that other users cannot tamper with these SFRs.

FMT_MOF.1, FMT_MSA.3, FMT_SMR.3, limit the acceptable values for secure access and security data, and protects the SFRs dependent on those values from being bypassed.

FIA_UID.2 and FIA_UAU.2 support other actions that allow the user access to the TOE by restricting the actions that the user can take before being.

Enable Detection of Login and Attack of other SFRs

FAU_GEN.1 and FAU_SAR.1 support other functions by providing login control and monitoring functions that allow intrusion attacks to be detected, and allows notification of the Superuser to security alarms, and record those security alarms in the audit trail.

FPT_STM.1 supports the security alarm and audit functions by providing a reliable timestamp for the audit log messages.

Other Analyses Performed

The dependency analysis provided at Table 18 and the analyses provided in Table 19, Table 20 and Table 20 demonstrate that the IT security functions work together to satisfy the TSFs, that is, they demonstrate mutual support between function components.

By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

This analysis of the security functional and assurance requirements demonstrates that there are no conflicts between requirements. Therefore, the security requirements together form a mutually supportive and consistent whole.

8.3.4 Assurance Security Requirements Rationale

The table below shows that all Security Assurance Requirements (SARs) are met by the assurance measures.

Table 22 - Mapping of SARs to Assurance Measures

Security Assurance Requirements	Assurance Measures
ACM_CAP.2	CM_DOC
ADO_DEL.1	DEL_DOC
ADO_IGS.1	IGS_DOC
ADV_FSP.1	FUN_SPEC
ADV_HLD.1	HLD_DOC
ADV_RCR.1	RCR_DOC
AGD_ADM.1	ADMIN
AGD_USR.1	USER
ATE_COV.1	TEST_COV
ATE_FUN.1	TEST_DOC
ATE_IND.2	TEST_DOC
AVA_SOF.1	SOF_DOC

Security Assurance Requirements	Assurance Measures
AVA_VLA.1	VLA_DOC

Given that all security assurance requirements are met by at least one assurance measure and that the implementation of each assurance measure will be the subject of evaluation activities, it is concluded that all of the assurance measures will meet all of the security assurance requirements.

CC EAL2 provides design information down to the High-Level Design, which is sufficient for the completion of an analysis of the strength of function, independent, and developer testing of security functions and includes analysis of obvious vulnerabilities for the TOE. Therefore CC EAL2 provides consumers with a low to moderate level of independently assured security services and is considered an appropriate level of assurance for the TOE.

8.3.5 Strength of Function Claims

The minimum Strength of Function for the TOE is **SOF-Basic**.

The security functional requirement FIA_UAU.2 provides the basis for the password mechanism. Passwords are inherently probabilistic and as such require a strength of function claim. The strength of function of the password in the TOE is SOF-Basic. The strength of function claim is based on the correct administration of the TOE. The assumptions to support the SOF claim are A.NOEVIL, A.PERSONNEL and A.POLICY. These assumptions ensure that the TOE is configured correctly, that administrators are trusted personnel and assume the organization has appropriate security policies in place to protect its assets.

The TOE security function IA.MECHANISM inherits the SOF claim above, as it implements the password requirements from the relevant security functional requirements identified above.

The claim for SOF-Basic is appropriate for this TOE as it is sufficient to protect against an attacker with a low attack potential, i.e. attackers with high resources, high skill and low motivation. Additionally, it is consistent with the evaluation level of EAL 2 and the testing that is carried out for that level of assurance.

8.4 Rationale for Extensions

It was found to be necessary to include FAU_AUD.1 instead of FAU_GEN.1 as the requirements imposed by FAU_GEN.1 are not appropriate for the TOE. The TOE does

not record the startup and shutdown of audit functions as the TOE has no facility to shutdown the audit functionality. Additionally, the TOE is designed to remain operational at all times, making the requirement for audit of startup and shutdown redundant. In addition, FAU_AUD.1 is considered an appropriate explicitly stated IT security requirement since FAU_AUD.1 has:

- been modeled on the FAU_GEN.1 requirement;
- followed the formal CC requirement structure:
  - Class = FAU
  - Family = FAU_AUD
  - Component = FAU_AUD.1;
- been articulated similar to FAU_GEN.1, making it just as measurable so that compliance of the TOE to the requirement can be determined and systematically demonstrated;
- been expressed clearly and unambiguously; and
- ensured that the assurance requirements defined by EAL2 are still applicable.

8.4.1 Rationale for Explicitly Stated Requirements

It was found to be necessary to create FPT_STM_EXP.1, to specifically address the use of a NTP server as mechanism to synchronize time. FPT_STM.1 did not go far enough to address the role of an external trusted NTP server in the IT environment that is available to periodically synchronize the TOE's internal system clock, in response to requests from the TOE.

It was found to be necessary to create FTP_ITC_EXP.1 to specifically address use of the IT environment to support and preclude unauthorized access to TSF data. FTP_ITC.1 did not go far enough to address the role of DCC channels, which are overhead channels peculiar to SONET/SDH communications that are used by the TOE to transport security management data between nodes.

It was found to be necessary to create FTP_SEP_EXP.1 to specifically address use of the IT environment to protect the management interfaces. FTP_SEP.1 did not go far enough to address the role of MSPP line cards to protect the management interfaces of the TOE from unauthorized access from sources external to the trusted management network.

8.5 PP Claims Rationale

This ST makes no PP conformance claim therefore no rationale is required.

Appendix A – Acronyms & Glossary

Acronyms

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
CC	Common Criteria
CPU	Central Processing Unit
CTC	Cisco Transport Controller
DCC	Data Communications Channel
DCN	Data Communications Network
DLC	Data Link Connection
DSLAM	Digital Subscriber Line Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing
EAL	Evaluation Assurance Level
EMS	Element Management System
ESP	Encapsulating Security Payload
GUI	Graphical user Interface
HDLC	High-level Data Link Control
IAD	Integrated Access Device
IKE	Internet Key Exchange
IP	Internet Protocol
IT	Information Technology
ITU	International Telecommunications Union
LED	Light Emitting Diode
MML	Man Machine Language

MPLS	Multi Protocol Label Switching
MSPP	Multiservice Provisioning Platform
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance & Provisioning
OC	Optical Carrier
ONS	Optical Networking System
PP	Protection Profile
PoP	Point of Presence
RAM	Random Access Memory
SA	Shelf Assembly
SAN	Storage Area Network
SCL	System Communication Link
SDH	Synchronous Digital Hierarchy
SDRAM	Synchronous Dynamic Random Access Memory
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SONET	Synchronous Optical Network
ST	Security Target
STS-1	Synchronous Transport Signal 1
TCC2	Timing, Communications and Control Card, Version 2
TDM	Time Division Multiplexing

TL1	Transaction Language 1
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Glossary

AAA	The three centralized access control technologies referred to as AAA: Authentication, Authorization, and Auditing.
Add/Drop Terminal	Allows signal to be added into or dropped from of a SONET span.
DLC	A user connection to a network that can be thought of as virtual channel.
DCC	An overhead channel in a SONET ring that allows individual nodes to communicate control information to each other.
DSLAM	Device that combines and separates the different formats of communications contained in the carrier and routes them to their respective hosts.
DWDM	DWDM combines multiple optical signals so that they can be amplified as a group and transported over a single fiber to increase capacity.
IAD	An IAD is a customer premises device that provides access to wide area networks and the Internet. Specifically, it aggregates multiple channels of information including voice and data across a single shared access link to a carrier or service provider PoP (Point of Presence).

Node	Endpoint of a network connection or a junction common to two or more lines in a network. In this ST the term “node” refers to an ONS 15454.
OC-3	Optical Carrier 3 is SONET transmission speed of 255.52 Mbps.
SDH	A European family of digital carrier rates using optical signals over fiber.
SONET	High-speed synchronous network designed to run on optical fiber.
STM-1	SDH basic building block at rate of 155.52 Mbps.
STS-1	The electrical version of the SONET OC-1 level signal.