National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco ONS 15454 SONET Multiservice Provisioning Platform (MSPP) Release 4.1.3 and Cisco ONS 15454 SDH Multiservice Provisioning Platform (MSPP) Release 4.1.3

Report Number: **CCEVS-VR-05-0129**
Dated: **October 21, 2005**
Version: **1.5**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory, Sterling, VA
Dill, Kenneth
Musa, Maria
Squires, Alicia

Validation Personnel:
Kenneth Eggers, Orion Security Solutions
John Nilles, The Aerospace Corporation
Jeffrey Klingler, National Security Agency

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Optical Network System (ONS) 15454 Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH) Multiservice Provisioning Platform (MSPP) Release 4.1.3.

The evaluation of the Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during October 2005. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Cisco Systems, Inc. and the Decisive Analytics Corporation. The ETR and test report used in developing this validation report were written by Arca. The evaluation team determined the product to be CC Version 2.2, January 2004, Revision 256,Part 2 extended with NIAP Interpretation I-0432 applied and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2 have been met.

The ONS 15454 SONET/SDH MSPP application is a software application bound to a product-specific Timing, Communications, and Control, version 2 hardware card (TCC2) installed in a product-specific shelf assembly. The primary purpose of the product is to provide the underlying infrastructure for metropolitan/regional optical transport networks. The TOE is a subset of the components of the overall product and consists of the card responsible for control and administration of the optical transport network infrastructure. This subset includes the subcomponents of the TCC2 card that directly or indirectly support the TOE Security Functions (TSF), the ONS 15454 system software and the Real-Time Clock (RTC) subsystem. Figure 1 below illustrates the TOE.

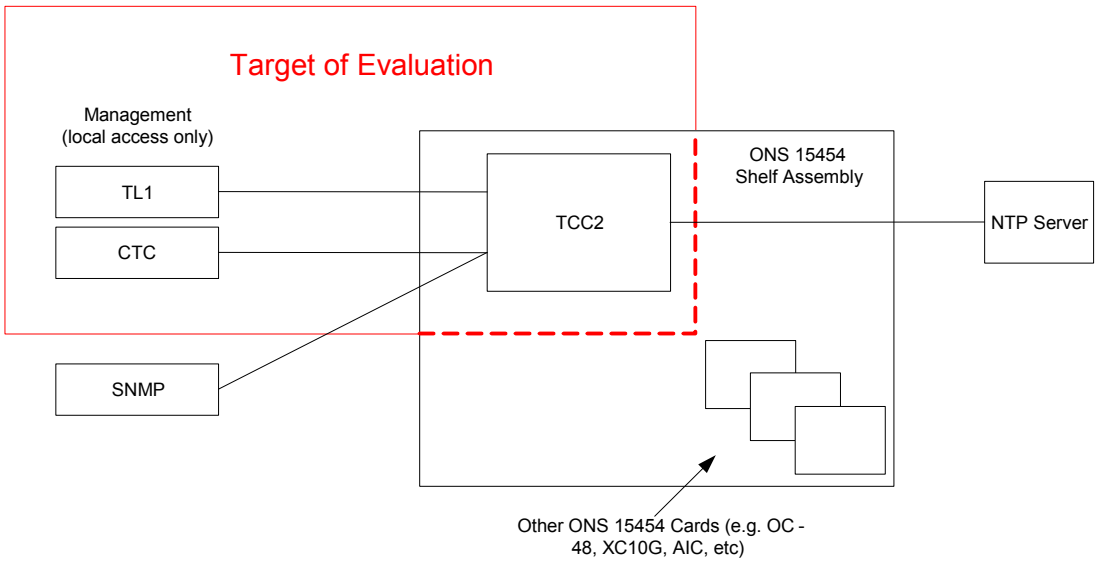

Figure 1 TOE as a Component of the ONS 15454

As is illustrated, the TOE is a component of a larger product. As such the TOE is reliant upon the protection mechanisms implemented by its IT environment (the rest of the ONS 15454 and physical protections). Therefore it is imperative that this product be installed and operated in the evaluated configuration. That configuration is described in the *Installation and Configuration Guide for the Common Criteria EAL2 Evaluated Cisco ONS 15454 SONET/SDH MSPP Release 4.1.3, V5*, dated 7 September 2005. In addition, the environment must satisfy the assumptions and provide the security functionality identified in the ST.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology [CEM] work unit verdicts), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2, with NIAP Interpretation I-0432 applied, evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

2 Identification

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Sponsors of information technology products who desire a security evaluation must contract with a CCTL to perform the evaluation. If the product successfully meets the evaluation requirements, it is listed on the NIAP Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The fully qualified identifier of the TOE as evaluated;
- The ST, describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	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) Specific product identification information is contained in *Table 3 - Hardware and Software Components*.
Security Target	Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Security Target, Revision 11, 19 October 2005
Evaluation Technical Report	• ACM_CAP.2 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V1, 15 September 2005 • ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V1, 15 September 2005 • ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V2, 18 October 2005 • AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V2, 18 October 2005 • ASE Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V2, 18 October 2005 • ATE_COV; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V1, 15 September 2005 • AVA_SOF.1; AVA_VLA.1 Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V1, 15 September 2005 • Evaluation Technical Report for Cisco ONS 15454 MSPP R4.1.3, V1, 16 September 2005
Conformance Result	CC Version 2.2, January 2004, Revision 256,Part 2 extended with NIAP Interpretation I-0432 applied, CC Part 3 conformant to EAL 2. No addition international interpretations.
Sponsor	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706
Interpretations	As in noted in the conformance results this evaluation included NIAP Interpretation I-0432 and international interpretations included in the January 2004 release of the CC version 2.2.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Arca Common Criteria Testing Laboratory 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validator(s)	Kenneth W. Eggers Orion Security Solutions, Inc. 4115 Earl Lee Cove Williamsburg, VA 23188-8026 John Nilles The Aerospace Corporation 8840 Stanford Boulevard, Suite 4400 Columbia, MD 21045

3 Security Policy

3.1 Identification and Authentication

The TOE requires each user to identify itself and provide authentication information before performing any other TSF-mediated action for the user. Upon receiving the user's ID and password, the TOE authenticates the user, based on the attributes, which are maintained for each individual user:

- User name,
- Password,
- Security level/privilege,
- Last login time and node,
- Number of failed logins, and
- Lockout status.

In the event that a user fails to authenticate more than a superuser-defined number (between 1 and 10) of times, the user's account is locked out until the superuser changes the account's lockout status.

3.2 Roles

Upon successful authentication, the TOE opens a session with the user at the security level/privilege associated with the user. The TOE permits a user to perform actions associated with a particular security level/privilege only if the user ID of the user is mapped to that security level/privilege's "role." The security level/privilege roles maintained by the TOE, in descending order of privilege, are:

- Superuser,
- Provisioning,
- Maintenance, and
- Retrieve.

The TOE limits the number of communication sessions per user on a given node to one and terminates inactive sessions to:

- 15 minutes for the superuser security level/privilege,
- 30 minutes for the provisioning security level/privilege,
- 60 minutes for the maintenance security level/privilege, and
- No limit for the retrieve security level/privilege.

3.3 Security Management

The TSF requires that the superuser security level/privilege be explicitly requested. The TSF restricts management of the following TOE management data to users assigned to the superuser security level/privilege:

- Functions that control user privileges;
- Functions that control session control parameters;
- Functions that control monitoring parameters;
- Maintenance of TSF configuration data;
- Specification of alternative initial values to override default values;
- Maintenance of user security attributes, such as:
  - Modification of user accounts,
  - Assignment of security level/privilege roles to user accounts, and
  - Setting security parameters; and
- Forcing logouts of other users.

3.4 Security Audit

The TOE maintains an audit trail that records the date, time, subject identity, and outcome of each of the following events:

- User login attempts,
- User logouts (including user logouts forced by the superuser),
- User lockout (exceeding the configured number of failed logins),
- User creation and deletion, and
- User privilege level modification.

3.5 Protection of the TSF

The TSF protects itself from interference and tampering by untrusted subjects and enforces separation among security domains for subjects under control of the TOE.

The TSF also provides reliable time stamps for its own use. The IT environment is required to provide a reliable time source for use by this time stamp function.

4 Assumptions

4.1 Physical Security Assumptions

- It is assumed that appropriate physical security controls, such as locating the TOE(s) in a secure communications room, securing the trusted Network Time Protocol (NTP) server, and the Data Communications Channel (DCC) links are implemented to protect the ONS 15454 installation from unauthorized access and modification.

- It is assumed that clock sources external to the scope of the TOE are in a secure location so as to provide a trusted clock source for the TOE's internal clock. This includes the TOE's RTC or the trusted NTP server located on a trusted network.

- It is assumed that the TOE is 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 the TSF and Organizational Security Policies (OSPs), thus only permitting access to Trusted TOE administrators. The trusted management network will contain the NTP server, and DCC links.

- It is assumed that ONS 15454 DCC connections are only made to other ONS 15454's in the CC-evaluated configuration.

- The TOE does not protect data traveling across the DCC link. It is assumed that data will be afforded appropriate protection by the Network owner such that data cannot be accessed in transit between network nodes.

4.2 Personnel Security Assumptions

- It is assumed that administrators of the TOE are non-hostile and trusted to perform their duties in a secure manner.
- It is assumed that administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

4.3 Clarification of Scope

The TOE is a subset of Cisco's ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3. The TOE consists of the TCC2 card and the ONS 15454 system software. The CTC application that is used to manage the ONS14545 is not part of the TOE. This is illustrated in Figure 1 above.

As a part of a larger system, the TOE is reliant upon the protection mechanisms implemented by the IT environment.

- The TOE does not protect administrative data (including administrator passwords) sent between nodes using DCC (fiber) connections. It relies upon the physical protection of the fiber connection to provide this protection.
- There are a number of services offered by the TOE, which are vulnerable to a malformed packet attack[1]. The TOE relies upon the physical protection of its management network and the isolation of that management network by other installed ONS 15454 cards.

[1] http://www.cisco.com/en/US/products/products_security_advisory09186a00802708da.shtml

Therefore it is imperative that this product be installed and operated in the evaluated configuration. That configuration is described in the *Installation and Configuration Guide for the Common Criteria EAL2 Evaluated Cisco ONS 15454 SONET/SDH MSPP Release 4.1.3, V5*, dated 7 September 2005. In addition, the environment must satisfy the assumptions and provide the security functionality identified in the ST.

5 Architectural Information

The TOE consists of the following components, which are a subset of the ONS 15454 product:

- Timing, Communications, and Control Card, Version 2.0
- ONS 15454 Management Subsystem
- RTC Subsystem

The remaining product components are excluded from the TOE. However, at a minimum a single SONET or SDH card is required to be installed.

5.1 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, Internet Protocol (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 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 NTP or Simple Network Time Protocol (SNTP) server. Further discussion on the physical scope of the TOE has been provided in section 2.2.

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.

5.2 ONS 15454 Management Subsystem

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:

- Transaction Language 1 (TL1): 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.

- Cisco Transport Controller (CTC): 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. However, the administrator is required to manage the TOE via the CTC application and/or the TL1 interface.

5.3 RTC Subsystem

The RTC subsystem is implemented by a real time clock chip on the TCC2 and is responsible for maintaining the system date and time. It is used by the processor to support the auditing security functions of the TOE (by providing a reliable time stamp). 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.

6 Documentation

Following is a list of documentation provided by the developer/vendor that should be used to configure and operate the TOE in a secure manner. Each document is identified by it title and part number. The most current versions each of these documents is generally on the documentation CD delivered with the ONS 15454 MSPP and that version should be used to configure and administer the TOE. The URLs below are provided for convenience and may not be up to date.

Common Criteria Specific Documentation

Installation and Configuration Guide for the Common Criteria EAL2 Evaluated Cisco ONS 15454 SONET/SDH MSPP Release 4.1.3, V5, 7 September 2005

Cisco ONS 15454 SONET/SDH MSPP Release 4.1.3 Security Target, V11, 19 October 2005

Cisco Administrative Guidance - Cisco ONS 15454 SONET

Cisco ONS 15454 Procedure Guide, Releases 4.1.x 1 and 4.
February 2004, Text Part Number: 78-15669-03 (Available on the product documentation CD.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c2001/ccmigration_09186a00801a5cfe.pdf

Cisco ONS 15454 Reference Manual, Releases 4.1.x 1 and 4.5
February 2004, Text Part Number: 78-15670-03 (Available on the product documentation CD.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c2001/ccmigration_09186a00801a42d2.pdf

Cisco ONS 15454 Troubleshooting Guide, Releases 4.1.x 1 and 4.5
February 2004, Text Part Number: 78-15671-03 (Available on the product documentation CD.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c2001/ccmigration_09186a00801a429a.pdf

Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 4.1.x 1 and 4.5
February 2004, Text Part Number: 78-15695-02 (Available on the product documentation CD.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c2001/ccmigration_09186a00801f97a8.pdf

Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Quick Reference Guide, Release 4.1.x 1 and 4.5
 February 2004, Text Part Number: 78-15696-01 (Available on the product documentation CD.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r4145doc/45tlqr.pdf

Cisco ONS 15454 and Cisco ONS 15327 TL1 for Beginners
 Text Part Number: 78-16097-01 (Available online only.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r46docs/tleasy01.pdf

Cisco ONS 15454 Release 4.1 Network Elements Defaults
July 2003, Text Part Number: 78-15775-01 (Available on the product documentation CD.)

Cisco ONS 15454 MSPP Engineering Planning Guide, Release 4.1 (Less Appendices A and D)
Dated August 2003 (Available online only.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c1609/ccmigration_09186a00801c7160.pdf

Release Notes for Cisco ONS 15454 Release 4.1.3
January 2004, Text Part Number: OL-4983-01 (Available online only.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/454relnt/454rn413.pdf

Cisco Administrative Guidance - Cisco ONS 15454 SDH

Cisco ONS 15454 SDH Procedure Guide, Releases 4.1 and 4.5,July2003
July 2003, Text Part Number: 75-15673-01 (Available on the product documentation CD.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2008/c2001/ccmigration_09186a00801a45d4.pdf

Cisco ONS 15454 SDH Reference Manual, Releases 4.1 and 4.5,July 2003
 July 2003, Text Part Number: 75-15674-01 (Available on the product documentation CD.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/454sdh45/r4145ref/sdhref45.pdf

Cisco ONS 15454 SDH Troubleshooting Guide, Releases 4.1 and 45,July 2003
July 2003, Text Part Number: 75-15672-01 (Available on the product documentation CD.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/454sdh45/r4145tbg/sdhtbs45.pdf\

Cisco ONS 15454 SDH Release 4.1 Network Element Defaults, July 2003
 July 2003, Text Part Number: 75-15774-01 (Available on the product documentation CD.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/454sdh45/sdhdft41.pdf

Cisco ONS 15454 MSPP Engineering Planning Guide, Release 4.1 (Less Appendices A and D)
Dated August 2003 (Available online only.)
http://www.cisco.com/application/pdf/en/us/guest/products/ps2010/c1609/ccmigration_09186a00801c7160.pdf

Release Notes for Cisco ONS 15454 SDH Release 4.1.3
January 2004, Text Part Number: OL-4983-01 (Available online only.)
http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/454relnt/454rn413.pdf

7 IT Product Testing

At EAL2 testing must demonstrate correspondence between the tests and the functional specification. Complete testing is not required; “the coverage analysis need not demonstrate that

all security functions have been tested, or that all external interfaces to the TSF have been tested."[2]

7.1 Developer Testing

The vendor testing included tests for each security function as listed:

- SM.ROLE – Security Management Roles;
- SM.SUPERUSER – Superuser Privilege Login;
- SM.MANAGE – Security Management;
- AA.EVENTS – Security Events;
- AA.AUDIT – Audit Trail;
- CM.CONTROLS – Login Controls;
- CM.MONITOR – Monitor User Sessions;
- IA.MECHANISM – Identification & Authentication Mechanism;
- SP.TIMESOURCE – Reliable Time Source; and
- SP.DOMAIN – Domain Separation.

7.2 Evaluation Team Independent Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation, and Startup documentation, and functional, independent, and vulnerability testing on the test configuration. The test configuration is depicted in Figure 3.

[2] CEM, V2.2. paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

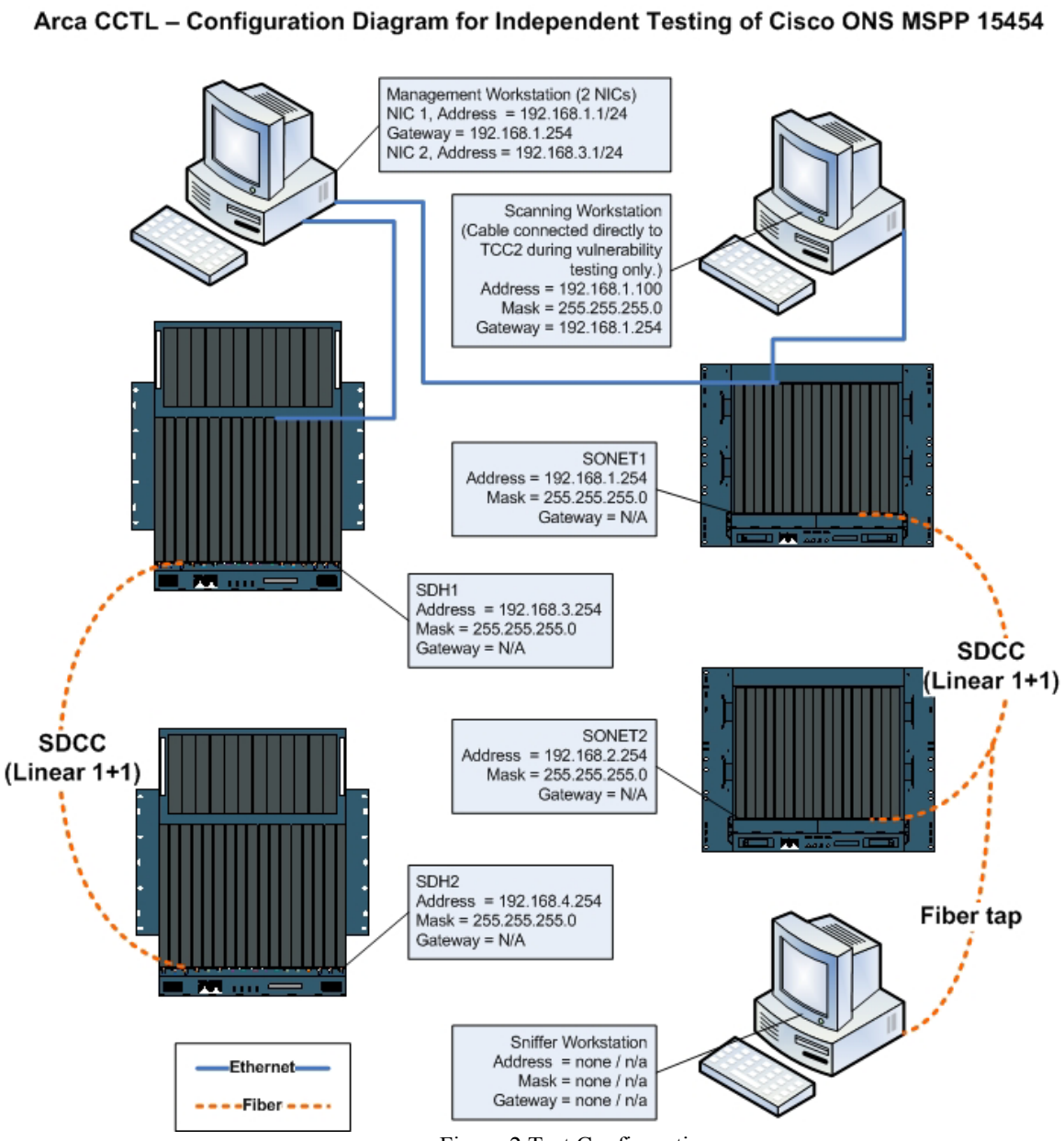

Figure 2 Test Configuration

In addition to the TOE hardware, a management workstation and two packet capture devices were used during testing. Those systems are identified in table 2.

Table 2 – Additional Test Equipment

System Configuration Name	Hardware Platform	Software Platform	NICS	RAM
Management Workstation	Intel	Windows 2000	3	256 MB
Sniffer (Ethernet)	Dell	Slackware 9.1	10/100	256 MB
Sniffer (Fiber)	SPARC	Solaris 8	2	256 MB

Evaluator testing covered the following areas:

- Storage of user attributes;
- Audit record generation;
- Concurrent session limitation;
- Enforcement of session timeouts;
- Enforcement of user lockout on authentication failures;
- Vulnerability scan; and
- Privilege escalation attack.

8 Evaluated Configuration

The evaluated configuration consisted of the components identified in the table below.

Table 3 - Hardware and Software Components

TOE Component	Part Number	Cisco Part Number, Revision
TOE Software	15454-0413-003L-1901 (SONET Compact Disc [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
	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)

9 Results of the Evaluation

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target.

- ACM: Configuration Management
    - ACM_CAP.2: Configuration items
- ADO: Delivery and Operation
    - ADO_DEL.1: Delivery procedures
    - ADO_IGS.1: Installation, generation, and start-up procedures
- ADV: Development
    - ADV_FSP.1: Informal functional specification
    - ADV_HLD.1: Descriptive high level design
    - ADV_RCR.1: Informal correspondence demonstration
- AGD: Guidance Documents
    - AGD_ADM.1: Administrator guidance
    - AGD_USR.1: User guidance
- ATE: Tests
    - ATE_COV.1: Evidence of coverage
    - ATE_FUN.1: Functional testing
    - ATE_IND.2: Independent testing - sample
- AVA: Vulnerability Assessment
    - AVA_SOF.1: Strength of TOE security function evaluation
    - AVA_VLA.1: Developer vulnerability analysis

10 Validator Comments

It is important to note that the TOE relies on protection mechanisms implemented by the IT environment to counter residual vulnerabilities. The environment via the isolation provided by installed ONS15454 communications cards and the protection of the fiber optic links between devices ensures this protection.

The residual vulnerabilities are malformed packet vulnerabilities, which could be used to cause a Denial of Service attack or otherwise compromise the TOE. These attacks are documented in the Cisco Security advisory - Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 Malformed Packet Vulnerabilities:

http://www.cisco.com/en/US/products/products_security_advisory09186a00802708da.shtml

These attacks are mitigated when the ONS is installed and operated the evaluated configuration.

11 Security Target

Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Security Target, Revision 11, 19 October 2005

12 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCTL	Common Criteria Testing laboratory
CD	Compact Disc
CEM	Common Evaluation Methodology
CTC	Cisco Transport Controller
DCC	Data Communications Channel
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTML	Hyper Text Markup Language
ID	Identifier
IP	Internet Protocol
MSPP	Multiservice Provisioning Platform
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Accreditation Program
ONS	Optical Networking System
OSP	Organizational Security Policies
RTC	Real-Time Clock
SDH	Synchronous Digital Hierarchy
SNTP	Simple **NTP**
SONET	Synchronous Optical Network
ST	Security Target
TCC2	Timing, Communications, and Control, version 2
TL1	Transaction Language 1
TOE	Target Of Evaluation
TSF	**TOE** Security Function
VR	Validation Report

13 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security, dated January 2004, version 2.2.

[6] Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Security Target, Revision 11, 19 October 2005

[7] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

14 Interpretations

14.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

No international interpretations beyond those incorporated into version CC version 2.2 were applied to Cisco ONS 15454 SONET/SDH Multiservice Provisioning Platform Release 4.1.3 Security Target:

14.2 NIAP Interpretations

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

- I-0432: List Of Subjects And Objects Refers To Types Thereof

14.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretation that it identified.