National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Ciena 6500 Packet Optical Platform

Report Number: **CCEVS-VR-VID11430-2025**

Dated: **January 02, 2025**

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt

Jenn Dotson

Linda Morrison

Clare Parran

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Furukh Siddique

Akshay Jain

Shaina Rae

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Ciena 6500 Packet Optical Platform Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in January 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The 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 Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

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

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- 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
TOE	Ciena 6500 Packet Optical Platform
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E]
Security Target	Ciena 6500 Packet Optical Platform Security Target v1.0
Evaluation Technical Report	Evaluation Technical Report for Ciena 6500 Packet Optical Platform, v0.9.
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor & Developer	Ciena Corporation
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Lauren Brandt, Jenn Dotson, Linda Morrison, Clare Parran, and Lori Sarem

3 Architectural Information

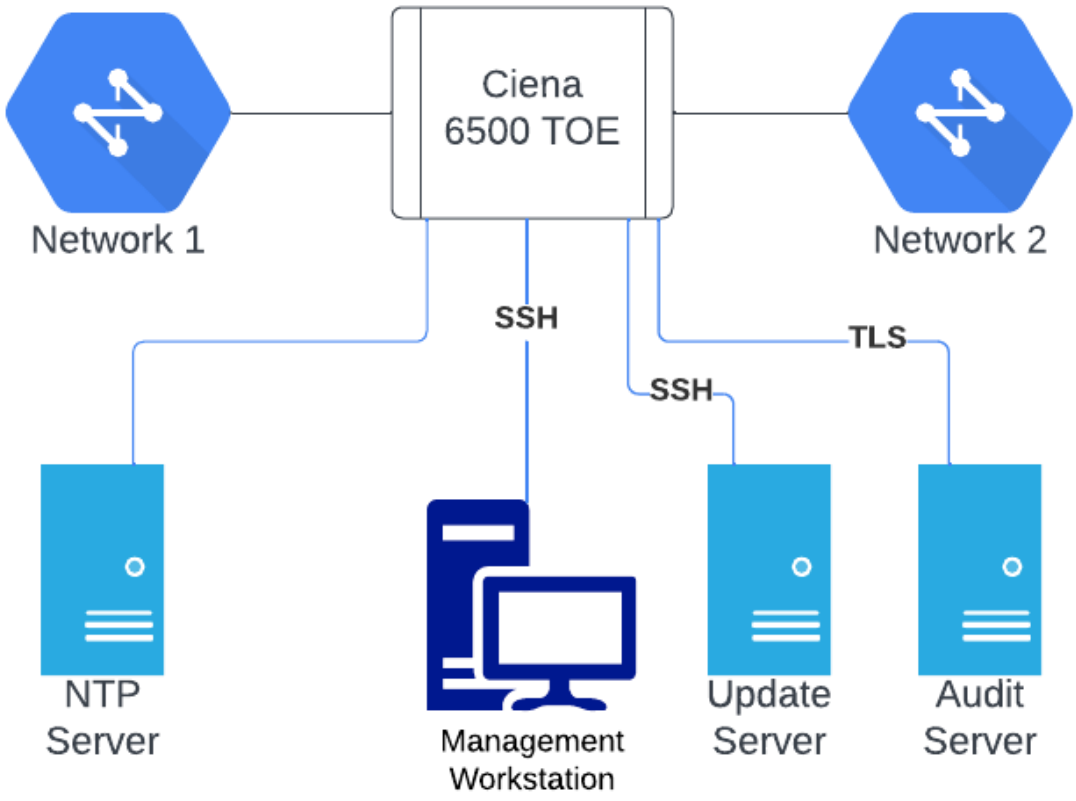
The TOE is the Ciena 6500 Packet Optical Platform running software version 15.6 and is developed by Ciena Corporation. The Ciena 6500 Packet Optical Platform, the Target of Evaluation (TOE), is a family of standalone hardware devices that run VxWorks and provide OSI Layers 1 and 2 network traffic management services. The security functions provided by the TOE include security auditing, cryptographic support, identification and authentication, security management, protection of TSF, TOE access controls, and trusted communications. The appliance provides the TL1 interface to the TOE's security management functionality. The TOE enables users to direct traffic to designated ports, giving them control of network availability for specific services. The system features an agnostic switch fabric that is capable of switching SONET/SDH, OTN, and Ethernet/MPLS networks. The switching behavior is beyond the scope of the claimed Protection Profile.

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. The Ciena 6500 has five shelf variants which range in size from 2RU (Rack Units) to 22RU (Rack Units). Each variant has the same software image loaded onto it and therefore each has the same security functionality across the family.

The five variants are:

- 6500-2
- 6500-4
- 6500-7
- 6500-14
- 6500-32

Figure 1 – Representative TOE Deployment



3.1 Physical Boundaries

The Physical boundary of the TOE is the Ciena 6500 Packet Optical Platform hardware appliance and the software which runs on it. The TOE runs VxWorks 6.9 for the SP3 and SPAP3 shelf processors. The TOE is managed using the Transaction Language 1 (TL1) interface, used for local or remote administration.

The TOE has two physical connections for security management: a local console (RJ-45 Craft ethernet port) for direct connections and a Central Office Local Area Network (COLAN) ethernet port for remote connections. An administrator can access the TL1 interface using either a local workstation connected directly to the TOE's Craft ethernet port or a remote workstation that can connect to the TOE over the COLAN ethernet via SSH. The TL1 interface is the command line interface for the TOE. The audit server communicates to the TOE via TLS; the update server communicates with the TOE using SFTP via SSH over the COLAN ethernet port. In practice, the TOE will be deployed to perform network switching functions and will be connected to a number of other pieces of network traffic infrastructure equipment. This has not been depicted in detail because this capability is out of scope of the TOE from a security functional perspective.

The TOE may consist of any of the following models:

Table 2: TOE Models

MODEL TYPE	MODEL PART #	SP3 Shelf Processor Card	SPAP3 Shelf Processor Card
2-slot Type 2	NTK503LA	NO	YES
4-slot Type	NTK503HA	YES	NO
7-slot	NTK503PA	YES	NO
7-slot type 2	NTK503KA	NO	YES
6500-7	NTK503RA	YES	NO
14-slot	NTK503BA NTK503CA NTK503CC NTK503GA NTK503AD NTK503BD NTK503CD NTK503SA	YES	NO
32-slot	NTK603AA NTK603AB	YES	NO

Models using the SP3 service card are running on QorIQ T1042 Quad Core processor, with VxWorks 6.9; models using SPAP3 Service Cards are running on QorIQ T1022 Dual Core processors with VxWorks 6.9. The TOE software version is 15.6.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

4.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE creates audit records for events related to security relevant events including authentication (success and failure, remote and local), cryptographic key management, session establishment (success and failure) and session termination, including for SSH communications. In addition, all actions corresponding to management functions are audited.

The TOE records, for each audited event, the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Depending on the specific type of event, additional data may be included in the audit record.

Audit data is stored locally transmitted in real-time to the remote audit server via TLS-protected trusted channel. The local audit data keeps the most recent records by overwriting the oldest records when the maximum size threshold of the file is met. No filesystem access is allowed to ensure protection of local audit data from deletion or modification.

4.2 Cryptographic Support

The TOE provides cryptography in support of SSH for remote administration, and secure download of TOE updates. The TOE provides a TLS protected channel for remote storage of audit data. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications. Cryptographic keys are overwritten by zeroes by the TOE when they are no longer needed for their purpose.

The TOE collects entropy from a local hardware entropy source contained within the device to ensure sufficient randomness for secure key generation.

The TOE utilizes a cryptographic module which can be referenced by its CAVP ID: #A5421.

4.3 Identification and Authentication

All users must be identified and authenticated by the TOE before being allowed to perform any actions on the TOE, except viewing a banner. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum-security strength through the set of supported characters and configurable minimum password length. As part of connecting to the TOE locally, using the management workstation, password data is obfuscated as it is inputted.

The TOE detects when a configurable number of failed authentication attempts are made by a remote user. Once this configurable threshold of between 2 and 20 attempts has been met the TSF will automatically lock a user's account. The user's account can be unlocked after a configurable time-period between 0 and 300 seconds or can be unlocked by a Security Administrator with sufficient User Privilege Code (UPC) level.

4.4 Security Management

The TSF provides the TL1 interface for performing management functions remotely or locally. Also, the Security Administrator can use the Site Manager to pass commands to the TL1 interface. The functions that a Security Administrator can perform on the TL1 interface are determined by the Security Administrator's UPC value. The Security Administrator is the only administrative role that has the ability to manage the TSF, so it is the only role that is within the scope of the TOE. Apart from the Security Administrator, other roles that perform network management related functionality are not considered part of the TSF.

4.5 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TSF prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-256. The TOE maintains system time with its local hardware clock and can synchronize with up to 3 NTPv4 time sources. TOE software updates are acquired using SFTP and initiated using the TL1 interface. Software updates are digitally signed to ensure their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

4.6 TOE Access

The TOE can terminate inactive sessions after a Security Administrator-configurable time period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE can also display a configurable banner on the TL1 interface that is displayed prior to use of any other security-relevant functionality.

4.7 Trusted Path/Channels

The Security Administrator establishes a trusted path to the TOE for remote administration using SSH. The TOE initiates a TLS-protected trusted channel to the remote audit data server. The TOE establishes a trusted channel (SSH) for downloading software updates from the update server using SSH.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

ID	Assumption
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

ID	Assumption
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND].

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Ciena 6500 Packet Optical Platform Security Target v1.0
- Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria Version 1.8
    - Externally Referenced Documents in the AGD
        - Ciena 6500 Packet-Optical Platform Administration and Security Release 15.6
        - Ciena 6500 Packet-Optical Platform TL1 Command Definition Release 15.6
        - Ciena 6500 Packet-Optical Platform User Interface Overview and Site Manager Fundamentals Release 15.6
        - Suite of Hardware Installation Manuals Release 15.6:
            - General Information
            - 2, 4, 7, 14, & 32 Slot Shelves (individual documents)

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 4 – Required Environmental Components

Component	Function
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications. Alternatively, the workstation can physically be connected to the TOE using the craft port, which is an Ethernet port through which the TOE can be managed locally using a SSH Client
Audit Server	A properly configured audit data storage server implementing the Syslog over TLS protocol.
Update Server	A server that supports SSH/SFTP and that is used as a location for storing product updates that can be transferred to the TOE.
Site Manager Software (Optional)	The Site Manager software provides a graphical interface to the TL1 interface for managing the TOE. The Site Manager software is installed on the Management workstation and uses an SSH channel to connect to the TOE.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

HTTP server, FTP service, Telnet and SNMP services – these must be disabled in the evaluated configuration. The TOE also includes a number of strictly unevaluated features and functions, which are outside the scope of the evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in ETR for Ciena 6500 Packet Optical Platform, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Ciena 6500 Packet Optical Platform that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND].

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of Development Documentation

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND] related to the examination of the information contained in the TOE Summary Specification.

The Validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of Guidance Documents

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND] related to the examination of the information contained in the operational guidance documents.

The Validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The Evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team performed the Assurance Activities in the Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in *the Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria*, Version 1.8, December 23, 2024. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 7.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the NDcPP 2.2e and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

- The security target is identified as: *Ciena 6500 Packet Optical Platform Security Target* v1.0, January 2025.

13 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.
- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.
- *Collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [PP-ND]
- *Ciena 6500 Packet Optical Platform Security Target*, v1.0, January 2025
- *Assurance Activity Report for Ciena 6500 Packet Optical Platform Version*, v0.8 January 2025 (AAR)
- *Evaluation Technical Report for Ciena 6500 Packet Optical Platform*, Version 0.9, January 2025
- *Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria*, Version 1.8, December 23, 2024